

# A Collapse Theorem for Holographic Algorithms with Matchgates on Domain Size At Most 4

Jin-Yi Cai\*

Zhiguo Fu†

## Abstract

Holographic algorithms with matchgates are a novel approach to design polynomial time computation. It uses Kasteleyn's algorithm for perfect matchings, and more importantly a holographic reduction. The two fundamental parameters of a holographic reduction are the domain size  $k$  of the underlying problem, and the basis size  $\ell$ . A holographic reduction transforms the computation to matchgates by a linear transformation that maps to (a tensor product space of) a linear space of dimension  $2^\ell$ . We prove a sharp basis collapse theorem, that shows that for domain size 3 and 4, all non-trivial holographic reductions have basis size  $\ell$  collapse to 1 and 2 respectively. The main proof techniques are Matchgate Identities, and a Group Property of matchgate signatures.

---

\*University of Wisconsin-Madison and Peking University. [jyc@cs.wisc.edu](mailto:jyc@cs.wisc.edu). Supported by NSF CCF-0914969 and NSF CCF-1217549.

†,Department of Computer Science and Engineering, Shanghai Jiao Tong University. [fuzg@sjtu.edu.cn](mailto:fuzg@sjtu.edu.cn)

# 1 Introduction

Matchgates were first introduced by Leslie Valiant [21] to show that a non-trivial, though restricted, fragment of quantum computation can be simulated in classical polynomial time. Subsequently he introduced holographic algorithms with matchgates [22] as a methodology to design polynomial time algorithms for some problems which seem to require exponential time. Computation in these algorithms is expressed and interpreted through a choice of linear basis vectors in an exponential “holographic” mix. Then the actual computation is carried out, via the Holant Theorem, by Kasteleyn’s algorithm (a.k.a. the FKT algorithm) [18, 19, 20] for counting the number of perfect matchings in a planar graph. This methodology has produced polynomial time algorithms for a number of problems, and minor variations of which are known to be NP-hard. The results are often surprising and counter-intuitive. For example, it is shown [23] that a restrictive SAT problem  $\#_7\text{Pl-Rtw-Mon-3CNF}$  (counting the number of satisfying assignments of a planar read-twice monotone 3CNF formula, modulo 7) is solvable in polynomial time. The same counting problem without mod 7 is known to be  $\#P$ -complete, thus fully general despite its apparent syntactic restriction; the problem mod 2 is  $\oplus P$ -complete, and thus NP-hard under randomized reductions. And yet, the problem mod 7 is tractable. Such “anomaly” challenges our conception of what polynomial time computation can do, and where the frontier between  $P$  and  $\#P$  lies, assuming they are truly different.

These holographic algorithms are quite exotic, and use a quantum-like superposition of fragments of computation to achieve a pattern of interference and cancellations. Since we lack any good absolute lower bounds that apply to unrestricted computational models, we should ask ourselves why do we believe those conjectures such as  $P \neq NP$  or  $P \neq P^{\#P}$  that are at the foundation of our discipline. We posit that the only defensible argument is the observed inability of existing algorithmic techniques to solve NP-hard or  $\#P$ -hard problems in polynomial time. Now these new holographic algorithms are quite unlike the existing algorithmic techniques, and thus pose a new challenge. To maintain the credibility of these widely believed conjectures, and the self-respect of the discipline, we must gain a better understanding of what the new methodology can or cannot do. To quote Valiant [22], “The most intriguing question, clearly, is whether polynomial time holographic algorithms exist for NP- or  $\#P$ -complete problems. . . . [T]he existence of such a reduction would be implied by the solvability of a finite system of polynomial equations . . . [A]ny proof of  $P \neq NP$  may need to explain, and not only to imply, the unsolvability of our polynomial systems.”

Substantial progress has been made. For example, the appearance of the modulus 7 for 3CNF, which was considered peculiar, has been “explained” by the fact that  $7 = 2^3 - 1$  is a Mersenne prime [4]. Thus, e.g.,  $\#_{31}\text{Pl-Rtw-Mon-5CNF}$  is in  $P$  by the same holographic algorithm. Such understanding is achieved only after a systematic study of the *structural theory* of holographic algorithms. This is the theory of what holographic reductions are possible, and what they can do with matchgates.

In the design of a holographic algorithm, a crucial step is a choice of linear basis vectors, through which the computation is expressed and interpreted. Because the underlying basic computation is ultimately reduced to perfect matchings, the linear basis vectors are of dimension  $2^\ell$ , where  $\ell$  is called the size of the basis. For a general CSP-type counting problem, one can assume there is a natural parameter  $k$ , called its domain size. This is the range over which variables take values. For example, Boolean CSP problems all have domain size 2. A  $k$ -coloring problem on graphs has domain size  $k$ . In holographic algorithms of domain size  $k$ , the linear basis has  $k$  vectors of dimension  $2^\ell$ , which can be expressed as a  $2^\ell \times k$  matrix.

Utilizing bases of an arbitrarily large but fixed size  $\ell$  is a theoretical possibility which may allow for an unlimited variety of holographic algorithms. For example, the algorithm for  $\#_7\text{Pl-Rtw-Mon-3CNF}$  in [23] originally used a basis of size  $\ell = 2$ , expressed as a  $4 \times 2$  matrix. However, over the Boolean domain ( $k = 2$ ), Cai and Lu [3] proved a surprising collapse theorem that *any* non-trivial holographic

algorithm on a basis of size  $\ell \geq 2$  can be simulated on a basis of size 1. (In particular, for  $\#_7\text{Pl-Rtw-Mon-3CNF}$ , there is a linear basis with 2 vectors of dimension  $2^1$ , expressed as a  $2 \times 2$  matrix.) This is the fundamental rationale to develop the theory for Boolean domain holographic algorithms over the group  $\mathbf{GL}_2(\mathbb{C})$  [4], which is the foundation for all the systematic results that have been achieved.

While this drastic collapse from an arbitrary  $2^\ell$  to 2 is surprising, perhaps there is a plausible philosophical justification. One might reason that for the Boolean domain  $k = 2$ , “information theoretically” one should need only 2 dimensions to encode data. (This is by no means a proof! It is technically false, as most philosophical arguments are, since provably there are holographic reductions in  $\mathbf{GL}_2(\mathbb{C})$  that cannot be done in  $\mathbf{GL}_2(\mathbb{R})$ .) Nevertheless, following this logic, an audacious but plausible conjecture is that for a general domain size  $k$ , there is a collapse to the smallest  $\ell$  such that  $2^\ell \geq k$ .

In this paper we prove a basis collapse theorem for holographic algorithms on domain size 3 and 4. For domain size 3, we show that all non-trivial holographic algorithms with matchgates using a basis of size  $\ell$  can be simulated by a basis of size 1. For domain size 4, we show that it collapses to size 2. Thus, for domain size 4, the proper transformation theory should be developed over the group  $\mathbf{GL}_4(\mathbb{C})$ . Note that there is a further surprise that the collapse for domain size 3 is not to dimension 4, but to dimension 2. This turns out to be a consequence of some very delicate properties of matchgates, philosophical arguments notwithstanding. In [24], Valiant gave holographic algorithms for several interesting problems on domain size 3. Holographic algorithms for domain size 4 or above are largely unexplored. The results of this paper are the first steps toward this goal. It shows that for domain size 4 we should develop the theory on  $\mathbf{GL}_4(\mathbb{C})$ , rather than on an infinite set of dimensions.

Our main proof techniques are Matchgate Identities, and a Group Property of matchgate signatures. A matchgate is a planar graph associated with a function called its (standard) signature, which represents its perfect matching properties. Matchgate Identities are a set of necessary and sufficient conditions for a matchgate (standard) signature. In [3], the proof of the collapse theorem on domain size 2 heavily depends on intricate constructions of matchgates; but this is difficult to generalize to domain size  $k > 2$ . Instead we introduce a new algebraic proof technique that heavily depends on Matchgate Identities. We will “construct” the required combinatorial objects—matchgates—by purely algebraic means. Starting from certain presumed holographic reductions, we will combine together algebraic objects, which we prove that they must correspond to matchgates. The most difficult step is to extract out a rank 4 submatrix of a certain signature matrix, using Matchgate Identities. In one crucial step we also use a Group Property that matchgate signatures satisfy, and use the algebraic inverse to obtain the combinatorial object. This indirect way of construction is similar to the way Gödel’s completeness theorem is proved (as simplified by Leon Henkin), where one builds a semantic object—a model—out of given syntactic objects, namely a consistent set of formulae. Our process is the reverse: We build concrete syntactic objects (matchgates) out of presumed semantic linear transformations.

This theory fits in a broader picture. Over the past few years a string of complexity dichotomy theorems have been proved [2, 5, 12, 13, 15, 6, 7, 10, 8, 9, 16, 17] which support parts of the following overall thesis: For a wide class of counting problems expressible as partition functions defined by local constraints, or sum-of-product computations, *every single problem* can be classified into one of three types. The first type is called tractable problems, which can be solved in polynomial time over arbitrary structures. The second type consists of problems that are  $\#P$ -hard over general structures, but solvable in polynomial time over planar structures. The third type problems are those which remain  $\#P$ -hard over planar structures. Moreover, the second type of problems are precisely those which are solvable by a holographic reduction to matchgates. Thus, the new methodology of holographic algorithms with matchgates constitutes a *universal* algorithm for all such problems. It is possible that the ultimate significance of this new methodology introduced by Valiant [22] lies in its pivotal rôle in this classification program. We note that for decades researchers in physics have studied the so-called “Exactly Solvable Models” (see e.g., [1]). The classification program, especially the universality part about the new

holographic algorithms with matchgates, if true, would provide an answer from computer science.

However, the provable part of this conjectured universality of holographic algorithms with matchgates is essentially restricted to the Boolean domain. The full scope of this thesis is beyond our ability to prove now. A main obstacle is that the theory of holographic algorithms with matchgates has not been adequately developed for domain size greater than 2. This paper is a necessary first step in that program.

This paper is organized as follows. In Section 2, we briefly give the background and some notations. In Section 3, we introduce degenerate and full rank signatures. In Section 4, we give a new algebraic proof for the collapse theorem on domain size 2, whereby introducing the new technique in a simpler setting. In Section 5, we give the collapse theorems on domain size 3 and 4. An illustrative problem solved by a holographic algorithm using matchgates on domain size 4 is given in the appendix.

## 2 Background and Notations

### 2.1 Background

In this section, we review some definitions and results. More details can be found in [22, 4].

A matchgate  $\Gamma$  is a triple  $(G, X, Y)$  where  $G$  is a planar embedding of a planar graph  $(V, E, W)$  where  $X \subseteq V$  is a set of input nodes and  $Y \subseteq V$  is a set of output nodes, and where  $X, Y$  are disjoint. Further, as one proceeds counterclockwise around the outer face starting from one point one encounters first the input nodes labeled  $1, 2, \dots, |X|$  and then the output nodes  $|Y|, \dots, 2, 1$  in that order. The arity of the matchgate is  $|X| + |Y|$ . For  $Z \subseteq X \cup Y$  we define the standard signature of  $\Gamma$  with respect to  $Z$  to be  $\text{PerfMatch}(G - Z)$ , where  $G - Z$  is the graph obtained by removing from  $G$  the node set  $Z$  and all edges that are incident to  $Z$ , and  $\text{PerfMatch}(G - Z)$  is the sum, over all perfect matchings  $M$  of  $G - Z$ , of the product of the weights of matching edges in  $M$ . Note that when all edges have weight 1, then  $\text{PerfMatch}(G)$  counts the number of perfect matchings. We define the standard signature of  $\Gamma$  to be the following  $2^{|Y|} \times 2^{|X|}$  matrix  $\underline{\Gamma}$  row-indexed by output nodes and column-indexed by input nodes (note that in [22],  $\underline{\Gamma}$  is a  $2^{|X|} \times 2^{|Y|}$  matrix row-indexed by input nodes and column-indexed by output nodes). The entries of  $\underline{\Gamma}$  are standard signatures of  $\Gamma$  with respect to  $Z$  for the  $2^{|X|+|Y|}$  choices of  $Z$ . The labeling of the matrix is as follows: Suppose that  $X$  and  $Y$  have the labeling described, i.e., the nodes are labeled  $1, 2, \dots, |X|$  and  $|Y|, \dots, 2, 1$  in counterclockwise order. Then each choice of  $Z$  is a subset of  $X \cup Y$ . If each node present in  $Z$  is denoted by a bit 1, and each node absent by a bit 0, then we have two binary strings in  $\{0, 1\}^{|X|}$  and  $\{0, 1\}^{|Y|}$  respectively, where the nodes labeled 1 (for both  $X$  and  $Y$ ) correspond to the leftmost binary bit. Suppose that  $i, j$  are the numbers represented by these strings in binary. Then the entry corresponding to  $Z$  will be the one in row  $i$  and column  $j$  in the signature matrix  $\underline{\Gamma}$ . This label ordering will allow the planar composition of matchgates connecting input nodes of one with the output nodes of another nicely correspond to matrix product.

A matchgate  $\Gamma$  is an odd (resp. even) matchgate if it has an odd (resp. even) number of nodes.

Let  $\Gamma$  be a matchgate. If  $\Gamma$  has no input nodes, then it is called a generator matchgate. If  $\Gamma$  has no output nodes, then it is called a recognizer matchgate. Otherwise  $\Gamma$  is called a transducer matchgate. Note that the standard signature  $\underline{G}$  of a generator matchgate is a column vector and the standard signature  $\underline{R}$  of a recognizer matchgate is a row vector.

From the definition of standard signatures, we directly have the following Lemma.

**Lemma 2.1.** *Let  $\underline{R}$  be the standard signature of a recognizer matchgate of arity  $n\ell$  and  $T$  be the standard signature of a transducer matchgate of  $\ell$ -output and  $s$ -input, then  $\underline{R}' = \underline{R}T^{\otimes n}$  is the standard signature of a recognizer matchgate of arity  $ns$ .*

On the other hand, we can view the standard signature of an  $n$ -output generator matchgate as a contravariant tensor  $\mathbf{G}$  with  $n$  (upper) indices. Under the standard basis  $[e_0 \ e_1] = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , it takes the form  $\underline{G}$  with  $2^n$  entries, where

$$\underline{G}^{i_1 i_2 \dots i_n} = \text{PerfMatch}(G - Z), \quad i_1, i_2, \dots, i_n \in \{0, 1\}.$$

Here  $Z$  is the subset of the output nodes having the characteristic sequence  $\chi_Z = i_1 i_2 \dots i_n$ , in which  $i_j$  is the bit for the output node labeled  $j$ , and  $G - Z$  is the graph obtained from  $G$  by removing  $Z$  and its incident edges. Then the column vector  $\underline{G} = (\underline{G}^{i_1 i_2 \dots i_n})$  whose entries are ordered lexicographically according to  $\chi_Z$  is the standard signature of a generator matchgate.

Similarly a recognizer matchgate with  $n$  input nodes is assigned a covariant tensor  $\mathbf{R}$  with  $n$  (lower) indices. Under the standard basis  $[e_0 \ e_1]$ , it takes the form  $\underline{R}$  with  $2^n$  entries,

$$\underline{R}_{i_1 i_2 \dots i_n} = \text{PerfMatch}(G - Z), \quad i_1, i_2, \dots, i_n \in \{0, 1\},$$

where  $Z$  is the subset of the input nodes having the characteristic sequence  $\chi_Z = i_1 i_2 \dots i_n$ . Then the row vector  $\underline{R} = (\underline{R}_{i_1 i_2 \dots i_n})$  whose entries are ordered lexicographically according to  $\chi_Z$  is the standard signature of a recognizer matchgate.

A basis  $M = (m_1, m_2, \dots, m_k)$  contains  $k$  vectors, each of them has dimension  $2^\ell$  (size  $\ell$ ). We use the following notation:  $M = (a_i^\alpha)$ , where lower index  $i \in [k]$  is for column and upper index  $\alpha \in \{0, 1\}^\ell$  is for row. A basis  $M$  need not be linearly independent. We say  $M$  has full rank if  $\text{rank}(M) = k$ . In the present paper, we assume that  $M$  has full rank (thus  $2^\ell \geq k$ ) unless otherwise specified.

Under a basis  $M$ , we can talk about the signature of a matchgate after the transformation.

**Definition 2.1.** The contravariant tensor  $\mathbf{G}$  of a generator matchgate  $\Gamma$  of arity  $n$  has signature  $G$  (written as a column vector) under basis  $M$  iff  $M^{\otimes n} \mathbf{G} = \underline{G}$  is the standard signature of the generator matchgate  $\Gamma$ .

**Definition 2.2.** The covariant tensor  $\mathbf{R}$  of a recognizer matchgate  $\Gamma'$  of arity  $n$  has signature  $R$  (written as a row vector) under basis  $M$  iff  $\underline{R} M^{\otimes n} = R$  where  $\underline{R}$  is the standard signature of the recognizer matchgate  $\Gamma'$ .

**Definition 2.3.** A contravariant tensor  $\mathbf{G}$  (resp. a covariant tensor  $\mathbf{R}$ ) is realizable over a basis  $M$  iff there exists a generator matchgate  $\Gamma$  (resp. a recognizer matchgate  $\Gamma'$ ) such that  $G$  (resp.  $R$ ) is the signature of  $\Gamma$  (resp.  $\Gamma'$ ) under basis  $M$ . They are simultaneously realizable if they are realizable over a common basis.

**Remark 1.** Under a basis of size  $\ell$ , if a general signature has arity  $n$ , then the standard signature is of arity  $n\ell$ , where  $n\ell$  is the number of external nodes in the matchgate. So a standard generator signature  $\underline{G}$  (resp. a standard recognizer signature  $\underline{R}$ ) has  $2^{n\ell}$  entries. We use  $\underline{G}^{\alpha_1 \alpha_2 \dots \alpha_n}$ , where each  $\alpha_i \in \{0, 1\}^\ell$ , to denote the blockwise form of the signature entry of  $\underline{G}$  of arity  $n\ell$ . Similarly we use the notation  $\underline{R}_{\alpha_1 \alpha_2 \dots \alpha_n}$  for a recognizer signature.

Then we have

$$\underline{G}^{\alpha_1 \alpha_2 \dots \alpha_n} = \sum_{j_1, j_2, \dots, j_n \in [k]} G^{j_1 j_2 \dots j_n} a_{j_1}^{\alpha_1} a_{j_2}^{\alpha_2} \dots a_{j_n}^{\alpha_n},$$

where  $\alpha_i \in \{0, 1\}^\ell$ , for  $i = 1, 2, \dots, n$ .

$$R_{j_1 j_2 \dots j_n} = \sum_{\alpha_1, \alpha_2, \dots, \alpha_n \in \{0, 1\}^\ell} \underline{R}_{\alpha_1 \alpha_2 \dots \alpha_n} a_{j_1}^{\alpha_1} a_{j_2}^{\alpha_2} \dots a_{j_n}^{\alpha_n},$$

where  $j_i \in [k]$ , for  $i = 1, 2, \dots, n$ .

A matchgrid  $\Omega = (A, B, C)$  is a weighted planar graph consisting of a disjoint union of: a set of (not necessarily distinct)  $g$  generator matchgates  $A = \{A_1, A_2, \dots, A_g\}$ , a set of (not necessarily distinct)  $r$  recognizer matchgates  $B = \{B_1, B_2, \dots, B_r\}$ , and a set of  $f$  connecting edges  $C = \{C_1, C_2, \dots, C_f\}$ , where each  $C_i$  edge has weight 1 and joins an output node of a generator matchgate with an input node of a recognizer matchgate, so that every input and output node in every constituent matchgate has exactly one such incident connecting edge.

Let  $G(A_i, M)$  be the signature of generator matchgate  $A_i$  under the basis  $M$  and  $R(B_j, M)$  be the signature of recognizer matchgate  $B_j$  under the basis  $M$ . Let  $G = \bigotimes_{i=1}^g G(A_i, M)$  and  $R = \bigotimes_{j=1}^r R(B_j, M)$  be their tensor product, then  $\text{Holant}(\Omega)$  is defined to be the *contraction* of these two product tensors (the sum over all indices of the product of the corresponding values of  $G$  and  $R$ ), where the corresponding indices match up according to the  $f$  connecting edges in  $C$ .

Valiant's Holant Theorem is

**Theorem 2.1.** (Valiant [22]) *For any matchgrid  $\Omega$  over any basis  $M$ , let  $\Gamma$  be its underlying weighted graph, then*

$$\text{Holant}(\Omega) = \text{PerfMatch}(\Gamma).$$

The FKT algorithm can compute the weighted sum of perfect matchings  $\text{PerfMatch}(\Gamma)$  for a planar graph in polynomial time. So  $\text{Holant}(\Omega)$  is computable in polynomial time.

## 2.2 Matrix Form of Signatures

**Definition 2.4.** *For a generator signature  $G = (G^{j_1 j_2 \dots j_n})$  on domain size  $k$ , the  $t$ -th matrix form  $G(t)$  ( $1 \leq t \leq n$ ) is a  $k \times k^{n-1}$  matrix, where the rows are indexed by  $1 \leq j_t \leq k$  and the columns are indexed by  $j_1 \dots j_{t-1} j_{t+1} \dots j_n$  in lexicographic order.*

**Definition 2.5.** *For a recognizer signature  $R = (R_{j_1 j_2 \dots j_n})$  on domain size  $k$ , the  $t$ -th matrix form  $R(t)$  ( $1 \leq t \leq n$ ) is a  $k^{n-1} \times k$  matrix where the rows are indexed by  $j_1 \dots j_{t-1} j_{t+1} \dots j_n$  in lexicographic order and the columns are indexed by  $1 \leq j_t \leq k$ .*

For example, let  $G = (G^{j_1 j_2})$  and  $R = (R_{j_1 j_2})$  where  $n = 2$  and  $k = 3$ , then

$$G(1) = \begin{pmatrix} G^{11} & G^{12} & G^{13} \\ G^{21} & G^{22} & G^{23} \\ G^{31} & G^{32} & G^{33} \end{pmatrix}, \quad R(1) = \begin{pmatrix} R_{11} & R_{21} & R_{31} \\ R_{12} & R_{22} & R_{32} \\ R_{13} & R_{23} & R_{33} \end{pmatrix},$$

We may consider a standard signature of arity  $n\ell$  as a signature on domain size  $k = 2^\ell$ , with the identity matrix  $I_{2^\ell}$ , then the following are special cases of Definition 2.4 and 2.5.

The  $t$ -th matrix form  $\underline{G}(t)$  ( $1 \leq t \leq n$ ) of the standard signature  $\underline{G} = (\underline{G}^{\alpha_1 \alpha_2 \dots \alpha_n})$  of a generator matchgate of arity  $n\ell$  is a  $2^\ell \times 2^{(n-1)\ell}$  matrix. Its rows are indexed by  $\alpha_t$  and its columns are indexed by  $\alpha_1 \dots \alpha_{t-1} \alpha_{t+1} \dots \alpha_n$ . The  $t$ -th matrix form  $\underline{R}(t)$  ( $1 \leq t \leq n$ ) of the standard signature  $\underline{R} = (\underline{R}_{\alpha_1 \alpha_2 \dots \alpha_n})$  of a recognizer matchgate of arity  $n\ell$  is a  $2^{(n-1)\ell} \times 2^\ell$  matrix. Its rows are indexed by  $\alpha_1 \dots \alpha_{t-1} \alpha_{t+1} \dots \alpha_n$  and its columns are indexed by  $\alpha_t$ . For example, let  $\underline{G} = (\underline{G}^{\alpha_1 \alpha_2})$ ,  $\underline{R} = (\underline{R}_{\alpha_1 \alpha_2})$  where  $n = 2, \ell = 2$ , then

$$\underline{G}(1) = \begin{pmatrix} \underline{G}^{0000} & \underline{G}^{0001} & \underline{G}^{0010} & \underline{G}^{0011} \\ \underline{G}^{0100} & \underline{G}^{0101} & \underline{G}^{0110} & \underline{G}^{0111} \\ \underline{G}^{1000} & \underline{G}^{1001} & \underline{G}^{1010} & \underline{G}^{1011} \\ \underline{G}^{1100} & \underline{G}^{1101} & \underline{G}^{1110} & \underline{G}^{1111} \end{pmatrix}, \quad \underline{R}(1) = \begin{pmatrix} \underline{R}_{0000} & \underline{R}_{0100} & \underline{R}_{1000} & \underline{R}_{1100} \\ \underline{R}_{0001} & \underline{R}_{0101} & \underline{R}_{1001} & \underline{R}_{1101} \\ \underline{R}_{0010} & \underline{R}_{0110} & \underline{R}_{1010} & \underline{R}_{1110} \\ \underline{R}_{0011} & \underline{R}_{0111} & \underline{R}_{1011} & \underline{R}_{1111} \end{pmatrix}.$$

The following lemma can be proved directly.

**Lemma 2.2.** *If  $\underline{G} = M^{\otimes n}G$ , where  $M$  is a  $2^\ell \times k$  basis,  $G$  is a generator signature of dimension  $k^n$ , then*

$$\underline{G}(t) = MG(t)(M^T)^{\otimes(n-1)}.$$

Denote the Hamming weight of a binary string  $\alpha$  as  $\text{wt}(\alpha)$ . We denote the row of  $\underline{G}(t)$  indexed by  $\alpha \in \{0,1\}^\ell$  as  $\underline{G}(t)^\alpha$ . The parity of  $\text{wt}(\alpha)$  is also called the parity of  $\underline{G}(t)^\alpha$ . The  $n \times n$  identity matrix is denoted as  $I_n$ . The transpose of the matrix  $A$  is denoted as  $A^T$ .

### 2.3 Matchgate Identities

Let  $\underline{G}$  be the standard signature of a matchgate of arity  $n$  (we discuss  $\underline{G}$  here, it is the same for  $\underline{R}$ ). A pattern  $\alpha$  is an  $n$ -bit string, i.e.,  $\alpha \in \{0,1\}^n$ . A position vector  $P = \{p_1, \dots, p_s\}$  is a subsequence of  $\{1, 2, \dots, n\}$ , where  $p_i \in [n]$  and  $p_1 < p_2 < \dots < p_s$ . A position vector  $P$  also denotes the pattern  $p$  whose  $(p_1, p_2, \dots, p_s)$ -th bits are 1 and others are 0. Let  $e_i \in \{0,1\}^n$  be the pattern with 1 in the  $i$ -th bit and 0 elsewhere. Let  $\alpha \oplus \beta$  be the bitwise XOR pattern of  $\alpha$  and  $\beta$ . Then for any pattern  $\alpha \in \{0,1\}^n$  and any position vector  $P = \{p_1, \dots, p_s\}$ , we have the following Matchgate Identities (MGI):

$$\sum_{i=1}^s (-1)^i \underline{G}^{\alpha \oplus e_{p_i}} \underline{G}^{\alpha \oplus p \oplus e_{p_i}} = 0. \quad (2.1)$$

By the definition of standard signatures, if  $\underline{G}$  is the standard signature of an odd matchgate, then  $\underline{G}^\alpha = 0$  for even  $\text{wt}(\alpha)$ . If  $\underline{G}$  is the standard signature of an even matchgate, then  $\underline{G}^\alpha = 0$  for odd  $\text{wt}(\alpha)$ . This is the Parity Condition of standard signatures.

**Theorem 2.2.** *A vector in  $\mathbb{C}^{2^n}$  is the standard signature of a matchgate iff it satisfies:*

- the Parity Condition,
- the Matchgate Identities.

For a proof see [11]. Actually in [11] it is shown that MGI implies the Parity Condition. But in practice, it is easier to apply the Parity Condition first. From the definition of MGI, we directly have the following lemma.

**Lemma 2.3.** *In MGI, the XOR of the indices in every product term  $\underline{G}^{\alpha \oplus e_i} \underline{G}^{\alpha \oplus p \oplus e_i}$  is the pattern  $p$ . Assume  $\underline{G}$  satisfies the Parity Condition. If  $\text{wt}(p)$  is odd, or if  $\text{wt}(p) = 2$ , then the MGI are automatically satisfied.*

*Proof.* The first statement is obvious. Hence if  $\text{wt}(p)$  is odd, then every product term is zero by the Parity Condition. If  $\text{wt}(p) = 2$ , then for any pattern  $\alpha$ , the matchgate identity is  $\underline{G}^{\alpha \oplus e_{p_1}} \underline{G}^{\alpha \oplus e_{p_2}} - \underline{G}^{\alpha \oplus e_{p_2}} \underline{G}^{\alpha \oplus e_{p_1}} = 0$ , so it is automatically satisfied.  $\square$

**Lemma 2.4.** *A signature  $G = (G^{i_1 i_2 i_3 i_4})$  of arity 4 is the standard signature of an even matchgate (generator or recognizer) iff  $G^\alpha = 0$  for all odd  $\text{wt}(\alpha)$  and*

$$G^{0000}G^{1111} - G^{1100}G^{0011} + G^{1010}G^{0101} - G^{1001}G^{0110} = 0. \quad (2.2)$$

*Similarly, it is the standard signature of an odd matchgate (generator or recognizer) iff  $G^\alpha = 0$  for all even  $\text{wt}(\alpha)$  and*

$$G^{1000}G^{0111} - G^{0100}G^{1011} + G^{0010}G^{1101} - G^{0001}G^{1110} = 0. \quad (2.3)$$

*Proof.* We prove the Lemma for the even case. The proof for the odd case is similar and we omit it.

If  $G = (G^{i_1 i_2 i_3 i_4})$  is the standard signature of an even matchgate, then  $G^\alpha = 0$  for odd  $\text{wt}(\alpha)$  by the Parity Condition. Equation (2.2) follows from MGI where we choose the position vector  $P = \{1, 2, 3, 4\}$  and the pattern 1000.

Conversely,  $G$  satisfies the Parity Condition as given. For arity 4, Lemma 2.3 shows that the only non-trivial position vector is  $P = \{1, 2, 3, 4\}$ . It can be verified that for  $P = \{1, 2, 3, 4\}$  and any pattern, the MGI is equivalent to equation (2.2) for an even matchgate of arity 4. Hence  $G$  satisfies MGI, and thus it is a standard signature by Theorem 2.2.  $\square$

### 3 Degenerate and Full Rank Signatures

**Definition 3.1.** A signature  $G$  (generator or recognizer) on domain size  $k$  is degenerate iff  $G$  has the following form:

$$G = \gamma_1 \otimes \gamma_2 \otimes \cdots \otimes \gamma_n,$$

where  $\gamma_i$  are vectors of dimension  $k$ .

**Lemma 3.1.** A signature  $G$  on domain size  $k$  is degenerate iff  $\text{rank}(G(t)) \leq 1$  for  $1 \leq t \leq n$ .

*Proof.* We prove the lemma for generator signatures. The proof for recognizer signatures is similar.

Let  $G = (G^{i_1 i_2 \cdots i_n})$ , where  $i_t \in [k]$ . If there exists  $t \in [k]$  such that  $\text{rank}(G(t)) = 0$ , then  $G$  is identically zero and is degenerate obviously. If the matrix form  $G(t)$  has rank 1 for  $1 \leq t \leq n$ , we will prove the lemma by induction on the arity  $n$ .

For  $n = 2$ , let  $G(1)^i$  be the  $i$ -th row of the first matrix form  $G(1)$ , then there exists a non-zero row  $G(1)^j$ , where  $j \in [k]$ , and  $a_1, a_2, \dots, a_k \in \mathbb{C}$  such that  $G(1)^i = a_i G(1)^j$  for  $1 \leq i \leq k$  from  $\text{rank}(G(1)) = 1$ . Let  $\gamma_1 = (a_1, a_2, \dots, a_k)$ ,  $\gamma_2 = G(1)^j$ , then  $G = \gamma_1 \otimes \gamma_2$ .

Inductively we assume that the lemma has been proved for arity less than  $n$ . There exists a non-zero row  $G(1)^j$  and  $a_1, a_2, \dots, a_k \in \mathbb{C}$  such that  $G(1)^i = a_i G(1)^j$  for  $1 \leq i \leq k$  from  $\text{rank}(G(1)) = 1$ . Note that  $G(1)^j$  is a signature of arity  $n - 1$  and the matrix forms of  $G(1)^j$  are sub-matrices of the matrix forms of  $G$ , thus there exist vectors  $\gamma_2, \gamma_3, \dots, \gamma_n$  of dimension  $k$  such that  $G(1)^j = \gamma_2 \otimes \gamma_3 \otimes \cdots \otimes \gamma_n$  by induction. Let  $\gamma_1 = (a_1, a_2, \dots, a_k)$ , then  $G = \gamma_1 \otimes \gamma_2 \otimes \cdots \otimes \gamma_n$ .

Conversely, if  $G = \gamma_1 \otimes \gamma_2 \otimes \cdots \otimes \gamma_n$ , it is obvious that the matrix form  $G(t)$  has rank at most 1 for  $1 \leq t \leq n$ .  $\square$

**Definition 3.2.** For a non-degenerate signature  $G$  (generator or recognizer) on domain size  $k$ , if there exists  $t$  such that  $\text{rank}(G(t)) = k$ , then  $G$  is called a signature of full rank.

**Remark 2.** We will prove a collapse theorem for holographic algorithms which employs at least one generator signature of full rank. For example, we will prove: For domain size 3, any non-trivial holographic algorithm on a basis of size  $\ell \geq 2$  which employs at least one generator signature of full rank can be simulated on a basis of size 1. Any holographic algorithm using only degenerate generator signatures is trivial.

### 4 A New Proof for the Collapse Theorem on Domain Size 2

The following is a simple lemma from Linear Algebra.

**Lemma 4.1.** Let  $A, B, C$  be  $m \times n$ ,  $n \times s$ ,  $s \times t$  matrices respectively, where  $\text{rank}(A) = n$ ,  $\text{rank}(C) = s$ , then

$$\text{rank}(AB) = \text{rank}(B), \quad \text{rank}(BC) = \text{rank}(B).$$



We need to introduce a new notation for a splicing operation. Let  $\alpha \in \{0, 1\}^\ell$  and  $\beta \in \{0, 1\}^{(n-1)\ell}$ . Then we use  $\beta \curvearrowright_t \alpha$  to denote the binary string  $\alpha_1 \alpha_2 \cdots \alpha_n \in \{0, 1\}^{n\ell}$ , where for each  $i$ ,  $\alpha_i \in \{0, 1\}^\ell$ ,  $\alpha_t = \alpha$  and  $\alpha_1 \cdots \alpha_{t-1} \alpha_{t+1} \cdots \alpha_n = \beta$ . Similarly, we denote a position vector  $P$  as  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2 \cdots p_d)$ , where  $p_i$  is in the  $t$ -th block for  $1 \leq i \leq d$ , and  $q_j$  is in other blocks for  $1 \leq j \leq d'$ .

In this section, assume that the basis  $M$  is a  $2^\ell \times 2$  matrix of rank 2,  $G$  is a generator signature of arity  $n$  and full rank on domain size 2 (thus there exists  $t \in [n]$  such that  $\text{rank}(G(t)) = 2$ ), and  $\underline{G} = M^{\otimes n} G$  is a standard signature of arity  $n\ell$ . Note that if  $M$  has rank at most one, or if all generators used by a holographic algorithm are not of full rank (on domain size 2 this means they are all degenerate), then the Holant is trivial to compute and this is a trivial holographic algorithm.

From Lemma 2.2, we have  $\underline{G}(t) = MG(t)(M^T)^{\otimes(n-1)}$ . Then by Lemma 4.1,  $\text{rank}(\underline{G}(t)) = 2$ . Therefore we can define  $\sigma, \tau \in \{0, 1\}^\ell$  and  $\zeta, \eta \in \{0, 1\}^{(n-1)\ell}$  as follows:

- $\underline{G}(t)^\sigma$  and  $\underline{G}(t)^\tau$  are linearly independent,
- $\text{wt}(\sigma \oplus \tau) = \min_{u \neq v, u, v \in \{0, 1\}^\ell} \{\text{wt}(u \oplus v) \mid \underline{G}(t)^u \text{ and } \underline{G}(t)^v \text{ are linearly independent}\}.$

Let  $x_\beta = \left( \frac{\underline{G}^{\beta \curvearrowright_t \sigma}}{\underline{G}^{\beta \curvearrowright_t \tau}} \right)$ , then there exist  $\zeta, \eta$  such that:

- $x_\zeta$  and  $x_\eta$  are linearly independent,
- $\text{wt}(\zeta \oplus \eta) = \min_{u \neq v, u, v \in \{0, 1\}^{(n-1)\ell}} \{\text{wt}(u \oplus v) \mid x_u \text{ and } x_v \text{ are linearly independent}\}.$

By the definition of  $\sigma, \tau, \zeta, \eta$ , we directly have the following Lemma.

**Lemma 4.2.** *If there exists  $\alpha \in \{0, 1\}^\ell$  such that  $0 < \text{wt}(\sigma \oplus \alpha) < \text{wt}(\sigma \oplus \tau)$  and  $0 < \text{wt}(\alpha \oplus \tau) < \text{wt}(\sigma \oplus \tau)$ , then  $\underline{G}(t)^\alpha$  is identically zero. Similarly, If there exists  $\beta \in \{0, 1\}^{(n-1)\ell}$  such that  $0 < \text{wt}(\eta \oplus \beta) < \text{wt}(\eta \oplus \zeta)$  and  $0 < \text{wt}(\beta \oplus \zeta) < \text{wt}(\eta \oplus \zeta)$ , then  $x_\beta$  is identically zero.*

Let  $\zeta \oplus \eta = e_{q_1} \oplus e_{q_2} \oplus \cdots \oplus e_{q_{d'}}$ , and  $\sigma \oplus \tau = e_{p_1} \oplus e_{p_2} \oplus \cdots \oplus e_{p_d}$ .

**Remark 3.** *In this paper, we will repeatedly use the following method to construct MGI. For any given  $\sigma, \tau, \zeta, \eta$ , define  $\{p_1, p_2, \dots, p_d\}$  and  $\{q_1, q_2, \dots, q_{d'}\}$  as above.*

- *Let the position vector be  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2 \cdots p_d)$  and the pattern be  $\zeta \curvearrowright_t (\sigma \oplus e_{p_1})$ , where  $p_1$  is the first non-zero position of the  $t$ -th block. The other pattern is  $\eta \curvearrowright_t (\tau \oplus e_{p_1})$ . Then we will get a Matchgate Identity such that the product  $\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau}$  is term. Note that  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2 \cdots p_d)$  is the set of the non-zero positions of  $(\zeta \curvearrowright_t \sigma) \oplus (\eta \curvearrowright_t \tau)$ .*
- *Every bit position in  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2 \cdots p_d)$  corresponds to a product term. For the position  $p_i$  in the  $t$ -th block, the product term is  $\underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_1} \oplus e_{p_i})} \underline{G}^{\eta \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_i})}$ . Outside the  $t$ -th block, the product term has the form  $\underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})}$ .*
- *Separate out the product terms corresponding to the positions in the  $t$ -th block from the rest in MGI, we get the equation*

$$\sum_{i=1}^d (-1)^{i+1} \underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_1} \oplus e_{p_i})} \underline{G}^{\eta \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_i})} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})}),$$

where  $\pm$  depends on  $j$ , and if  $q_j$  occurs after the  $t$ -th block then it also depends on the parity of  $d$ . However this will not matter to us, since in this paper whenever we use this method we will show that these terms where we write an indefinite  $\pm$  sign all vanish.

**Lemma 4.3.** *The Hamming distance  $d$  between the minimizing  $\sigma$  and  $\tau$  is 1.*

*Proof.* For a contradiction assume  $d \geq 2$ . Let  $x_\zeta = \left( \frac{G^{\zeta \curvearrowright \sigma}}{G^{\zeta \curvearrowright \tau}} \right)$ ,  $x_\eta = \left( \frac{G^{\eta \curvearrowright \sigma}}{G^{\eta \curvearrowright \tau}} \right)$ . These are linearly independent by definition. We will prove that  $\underline{G}^{\zeta \curvearrowright \sigma} \underline{G}^{\eta \curvearrowright \tau} - \underline{G}^{\zeta \curvearrowright \tau} \underline{G}^{\eta \curvearrowright \sigma} = 0$  by MGI to get a contradiction.

We will apply MGI twice. The first time we use the pattern  $\zeta \curvearrowright (\sigma \oplus e_{p_1})$  with the position vector  $(q_1 q_2 \cdots q_{d'}) \curvearrowright (p_1 p_2 \cdots p_d)$ . Note that the other pattern obtained by XOR is  $\eta \curvearrowright (\tau \oplus e_{p_1})$ . This gives

$$\sum_{i=1}^d (-1)^{i+1} \underline{G}^{\zeta \curvearrowright (\sigma \oplus e_{p_1} \oplus e_{p_i})} \underline{G}^{\eta \curvearrowright (\tau \oplus e_{p_1} \oplus e_{p_i})} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})}), \quad (4.1)$$

The second time we use the same position vector  $(q_1 q_2 \cdots q_{d'}) \curvearrowright (p_1 p_2 \cdots p_d)$  with the pattern  $\zeta \curvearrowright (\tau \oplus e_{p_1})$ . Note that the other pattern obtained by XOR is  $\eta \curvearrowright (\sigma \oplus e_{p_1})$ . This gives

$$\sum_{i=1}^d (-1)^{i+1} \underline{G}^{\zeta \curvearrowright (\tau \oplus e_{p_1} \oplus e_{p_i})} \underline{G}^{\eta \curvearrowright (\sigma \oplus e_{p_1} \oplus e_{p_i})} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\sigma \oplus e_{p_1})}). \quad (4.2)$$

Note that (4.1) and (4.2) are symmetric: By switching  $\sigma$  and  $\tau$ , we will go from (4.1) to (4.2).

If  $d = 2$ , from (4.1), we have

$$\underline{G}^{\zeta \curvearrowright \sigma} \underline{G}^{\eta \curvearrowright \tau} - \underline{G}^{\zeta \curvearrowright \tau} \underline{G}^{\eta \curvearrowright \sigma} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})}).$$

From Lemma 4.2, by taking  $\alpha = \tau \oplus e_{p_1}$ , we get  $\underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})} = 0$  for  $1 \leq j \leq d'$ . Thus  $\underline{G}^{\zeta \curvearrowright \sigma} \underline{G}^{\eta \curvearrowright \tau} - \underline{G}^{\zeta \curvearrowright \tau} \underline{G}^{\eta \curvearrowright \sigma} = 0$ . This contradicts that  $x_\zeta = \left( \frac{G^{\zeta \curvearrowright \sigma}}{G^{\zeta \curvearrowright \tau}} \right)$  and  $x_\eta = \left( \frac{G^{\eta \curvearrowright \sigma}}{G^{\eta \curvearrowright \tau}} \right)$  are linearly independent, so  $d \neq 2$ .

If  $d > 2$ , then  $\underline{G}^{\zeta \curvearrowright (\sigma \oplus e_{p_1} \oplus e_{p_i})} = 0$  and  $\underline{G}^{\zeta \curvearrowright (\tau \oplus e_{p_1} \oplus e_{p_i})} = 0$ , for  $i > 1$  by Lemma 4.2. From (4.1) and (4.2), we have

$$\underline{G}^{\zeta \curvearrowright \sigma} \underline{G}^{\eta \curvearrowright \tau} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})}), \quad (4.3)$$

$$\underline{G}^{\zeta \curvearrowright \tau} \underline{G}^{\eta \curvearrowright \sigma} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\sigma \oplus e_{p_1})}). \quad (4.4)$$

In the right hand side of (4.3) and (4.4),  $\underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\tau \oplus e_{p_1})} = 0$ ,  $\underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright (\sigma \oplus e_{p_1})} = 0$  for  $1 \leq j \leq d'$  by Lemma 4.2, so  $\underline{G}^{\zeta \curvearrowright \sigma} \underline{G}^{\eta \curvearrowright \tau} = 0$  and  $\underline{G}^{\zeta \curvearrowright \tau} \underline{G}^{\eta \curvearrowright \sigma} = 0$ . This is also a contradiction to the linear independence of  $x_\zeta = \left( \frac{G^{\zeta \curvearrowright \sigma}}{G^{\zeta \curvearrowright \tau}} \right)$  and  $x_\eta = \left( \frac{G^{\eta \curvearrowright \sigma}}{G^{\eta \curvearrowright \tau}} \right)$ . It follows that  $d = 1$ .  $\square$

From Lemma 4.3, we have  $\sigma \oplus \tau = e_{p_1}$  and  $\zeta \oplus \eta = e_{q_1} \oplus e_{q_2} \oplus \cdots \oplus e_{q_{d'}}$ .

**Lemma 4.4.** *For the given  $\sigma$  and  $\tau$ , the Hamming distance  $d'$  between the minimizing  $\zeta$  and  $\eta$  is 1.*

*Proof.* For a contradiction assume  $d' \geq 2$ . We apply MGI twice, with the same position vector  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t p_1$  and the patterns  $\zeta \curvearrowright_t (\sigma \oplus e_{p_1}) = \zeta \curvearrowright_t \tau$  and  $\zeta \curvearrowright_t (\tau \oplus e_{p_1}) = \zeta \curvearrowright_t \sigma$  respectively.

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t \tau} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t \sigma}), \quad (4.5)$$

$$\underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t \sigma} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t \tau}). \quad (4.6)$$

By Lemma 4.2, we have  $\underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t \tau} = 0$  and  $\underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t \sigma} = 0$  for  $1 \leq j \leq d'$ . So  $\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} = 0$  and  $\underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = 0$ . This contradicts that  $x_\zeta = \begin{pmatrix} \underline{G}^{\zeta \curvearrowright_t \sigma} \\ \underline{G}^{\zeta \curvearrowright_t \tau} \end{pmatrix}$ ,  $x_\eta = \begin{pmatrix} \underline{G}^{\eta \curvearrowright_t \sigma} \\ \underline{G}^{\eta \curvearrowright_t \tau} \end{pmatrix}$  are linearly independent. Thus  $d' = 1$ .  $\square$

From Lemma 4.3 and Lemma 4.4 we have  $\sigma \oplus \tau = e_{p_1}$  and  $\zeta \oplus \eta = e_{q_1}$ .

The basis  $M$  is a  $2^\ell \times 2$  matrix with rows indexed by  $\alpha \in \{0, 1\}^\ell$ . Let  $M^\alpha$  denote the row with index  $\alpha$ . Let  $M^{\alpha_1, \alpha_2, \dots, \alpha_s}$  denote the sub-matrix of  $M$  whose rows are  $\alpha_1, \alpha_2, \dots, \alpha_s$ . Then we have the following corollary.

**Corollary 4.1.**  $M^{\sigma, \tau}$  is invertible.

*Proof.* Since  $\begin{pmatrix} \underline{G}^{\zeta \curvearrowright_t \sigma} & \underline{G}^{\eta \curvearrowright_t \sigma} \\ \underline{G}^{\zeta \curvearrowright_t \tau} & \underline{G}^{\eta \curvearrowright_t \tau} \end{pmatrix}$  is a sub-matrix of  $M^{\sigma, \tau} G(t) (M^T)^{\otimes (n-1)}$ ,  $M^{\sigma, \tau}$  has rank at least 2. Since  $M^{\sigma, \tau}$  is a  $2 \times 2$  matrix, it follows that  $M^{\sigma, \tau}$  has rank exactly 2 and is invertible.  $\square$

Note that  $(M^{\sigma, \tau})^{\otimes n} G$  is a column vector obtained by taking only entries of  $\underline{G}$  with index values either  $\sigma$  or  $\tau$ . It is a column vector of dimension  $2^n$  and we denote it by  $\underline{G}^{* \leftarrow \sigma, \tau}$ .

**Theorem 4.1.**  $\underline{G}^{* \leftarrow \sigma, \tau} = (M^{\sigma, \tau})^{\otimes n} G$  is the standard signature of a generator matchgate of arity  $n$  and  $\text{rank}(\underline{G}^{* \leftarrow \sigma, \tau}(t)) = 2$  for some  $t$ .

*Proof.* Let  $\Gamma$  be a matchgate realizing the standard signature  $\underline{G} = M^{\otimes n} G$ . Note that  $\Gamma$  has  $n\ell$  external nodes. For every block with  $\ell$  nodes, for  $1 \leq i \leq \ell$ , if the  $i$ -th bit of  $\sigma$  is 1 then we add an edge of weight 1 to the  $i$ -th external node, and the new node replaces it as an external node. If the  $i$ -th bit of  $\sigma$  is 0 then we do nothing to it. We get a new matchgate  $\Gamma'$ . Next, we define  $\Gamma''$  from  $\Gamma'$ : In each block of  $\ell$  external nodes of  $\Gamma'$ , we pick only the  $p_1$ -th external node as an external node of  $\Gamma''$ ; all others are considered internal nodes of  $\Gamma''$ . Then we get a matchgate  $\Gamma''$  realizing  $\underline{G}^{* \leftarrow \sigma, \tau} = (M^{\sigma, \tau})^{\otimes n} G$ . Note that all of the bits of  $\sigma, \tau$  are the same except the  $p_1$ -th bit. Since  $M^{\sigma, \tau}$  has rank 2,  $\underline{G}^{* \leftarrow \sigma, \tau}(t) = M^{\sigma, \tau} G(t) (M^{\sigma, \tau})^{T \otimes (n-1)}$  has rank 2 when  $G(t)$  has rank 2, by Lemma 4.1.  $\square$

Note that  $(M^{\sigma, \tau})^{\otimes (t-1)} \otimes M \otimes (M^{\sigma, \tau})^{\otimes (n-t)} G$  is a column vector of dimension  $2^{n+\ell-1}$  and we denote it by  $\underline{G}^{t^c \leftarrow \sigma, \tau}$ .

**Lemma 4.5.**  $\underline{G}^{t^c \leftarrow \sigma, \tau}$  is the standard signature of a generator matchgate of arity  $n + \ell - 1$ .

*Proof.* The proof of this lemma is similar to Theorem 4.1. Let  $\Gamma$  be a matchgate realizing the standard signature  $\underline{G} = M^{\otimes n} G$ .  $\Gamma$  has  $n\ell$  external nodes. We do nothing to the  $t$ -th block. For the other blocks, we add an edge of weight 1 to the  $i$ -th external node if the  $i$ -th bit of  $\sigma$  is 1 and do nothing to it if the  $i$ -th bit of  $\sigma$  is 0 for  $1 \leq i \leq \ell$ . Then we get a new matchgate  $\Gamma'$ . Now take the external nodes of  $\Gamma'$  in the  $t$ -th block, and the  $p_1$ -th external node in the other blocks, then we get a matchgate realizing  $\underline{G}^{t^c \leftarrow \sigma, \tau}$ .  $\square$

**Lemma 4.6.** Let  $\underline{G} = (\underline{G}^{i_1 i_2 \dots i_n})$  be the standard signature of a generator matchgate  $\Gamma$  of arity  $n$ . If  $\underline{G}$  has full rank and the  $t$ -th matrix form  $\underline{G}(t)$  has rank 2, then there exists a standard signature  $\underline{R}$  realized by a recognizer matchgate of arity  $n$  such that  $\underline{G}(t)\underline{R}(t) = I_2$ .

*Proof.* From Lemma 4.3 and Lemma 4.4, there is a sub-matrix  $A = \begin{pmatrix} \underline{G}^{\alpha \curvearrowright t 0} & \underline{G}^{\beta \curvearrowright t 0} \\ \underline{G}^{\alpha \curvearrowright t 1} & \underline{G}^{\beta \curvearrowright t 1} \end{pmatrix}$  of rank 2 in  $\underline{G}(t)$ , where  $\alpha, \beta \in \{0, 1\}^{n-1}$  and  $\text{wt}(\alpha \oplus \beta) = 1$ .

By the Parity Condition,  $\underline{G}^{\alpha \curvearrowright t 0} = \underline{G}^{\beta \curvearrowright t 1} = 0$  or  $\underline{G}^{\beta \curvearrowright t 0} = \underline{G}^{\alpha \curvearrowright t 1} = 0$ . We prove the Lemma for the case  $\underline{G}^{\beta \curvearrowright t 0} = \underline{G}^{\alpha \curvearrowright t 1} = 0$ , i.e,  $A = \begin{pmatrix} \underline{G}^{\alpha \curvearrowright t 0} & 0 \\ 0 & \underline{G}^{\beta \curvearrowright t 1} \end{pmatrix}$ . The other case is similar.

Let  $\underline{R}$  be a vector of dimension  $2^n$ , where

$$\begin{pmatrix} \underline{R}_{\alpha \curvearrowright t 0} & 0 \\ 0 & \underline{R}_{\beta \curvearrowright t 1} \end{pmatrix} = A^{-1},$$

and all other entries of  $\underline{R}$  are zero. It is obvious that  $\underline{G}(t)\underline{R}(t) = I_2$  (Note that  $\underline{R}(t)$  is a  $2^{n-2} \times 2$  matrix). Furthermore, there are only two non-zero entries in  $\underline{R}$  and the Hamming weight of XOR of their indices is 2, so it satisfies the Parity Condition and MGI by Lemma 2.3. Thus  $\underline{R}$  is a standard signature.  $\square$

Let  $T = M(M^{\sigma, \tau})^{-1}$ . Note that  $T^{\sigma, \tau} = I_2$ . Then

$$\underline{G} = M^{\otimes n} G = T^{\otimes n} (M^{\sigma, \tau})^{\otimes n} G = T^{\otimes n} \underline{G}^{* \leftarrow \sigma, \tau}$$

and from that,

$$\underline{G}^{t^c \leftarrow \sigma, \tau} = (T^{\sigma, \tau})^{\otimes (t-1)} \otimes T \otimes (T^{\sigma, \tau})^{\otimes (n-t)} \cdot \underline{G}^{* \leftarrow \sigma, \tau}.$$

The entries of  $\underline{G}^{t^c \leftarrow \sigma, \tau}$  can be indexed by  $i_1 \dots i_{t-1} i'_1 \dots i'_\ell i_{t+1} \dots i_n$ , where  $i_j, i'_{j'} \in \{0, 1\}$ . We denote the matrix form of  $\underline{G}^{t^c \leftarrow \sigma, \tau}$  by  $\underline{G}^{t^c \leftarrow \sigma, \tau}(t)$ , whose rows are indexed by  $i'_1 \dots i'_\ell$  and columns are indexed by  $i_1 \dots i_{t-1} i_{t+1} \dots i_n$ . Then by Lemma 2.2, we have

$$\underline{G}^{t^c \leftarrow \sigma, \tau}(t) = T \underline{G}^{* \leftarrow \sigma, \tau}(t) ((T^{\sigma, \tau})^T)^{\otimes (n-1)} = T \underline{G}^{* \leftarrow \sigma, \tau}(t). \quad (4.7)$$

**Lemma 4.7.**  $T$  is the standard signature of a transducer matchgate with  $\ell$ -output and 1-input.

*Proof.* By Theorem 4.1 and Lemma 4.6, there exists a standard signature of a recognizer matchgate  $\underline{R}$  such that  $\underline{G}^{* \leftarrow \sigma, \tau}(t) \underline{R}(t) = I_2$ . Let  $\Gamma_1$  be the matchgate realizing  $\underline{G}^{t^c \leftarrow \sigma, \tau}$  with output nodes  $X_1, \dots, X_{t-1}, Y_1, \dots, Y_\ell, Z_{t+1}, \dots, Z_n$ , and let  $\Gamma_2$  be the matchgate realizing  $\underline{R}$  with input nodes  $W_1, W_2, \dots, W_n$ . Then connect  $X_i$  with  $W_i$  for  $1 \leq i \leq t-1$  and  $Z_i$  with  $W_i$  for  $t+1 \leq i \leq n$  by an edge with weight 1 respectively, we get a transducer matchgate  $\Gamma$  with output nodes  $Y_1, Y_2, \dots, Y_\ell$  and input node  $X_t$ . Then  $T = \underline{G}^{t^c \leftarrow \sigma, \tau}(t) \underline{R}(t)$  is the standard signature of  $\Gamma$ . Note that all the connections are made respecting the planarity condition.  $\square$

The proof of Lemma 4.7 is illustrated by Fig. 1.

The following theorem is the main theorem in [3]; the algebraic method in this section gives a simpler proof. This method will be used in the next section to prove a similar collapse theorem for domain size 3 and 4.

**Theorem 4.2.** Any holographic algorithm on a basis of size  $\ell \geq 2$  and domain size 2 which employs at least one generator signature of full rank can be simulated on a basis of size 1.

*Proof.* Let  $\underline{R}_i M^{\otimes m_i} = R_i$  for  $1 \leq i \leq r$  and  $\underline{G}_j = M^{\otimes n_j} G_j$  for  $1 \leq j \leq g$ , where  $R_i, G_j$  are recognizer and generator signatures that a holographic algorithm employs and  $\underline{R}_i, \underline{G}_j$  are standard signatures. Without loss of generality, let  $G_1$  be of full rank. We define  $\sigma$  and  $\tau$  in terms of  $G_1$  and apply Corollary 4.1. The basis  $M$  has a full rank sub-matrix  $M^{\sigma, \tau}$ , where  $\text{wt}(\sigma \oplus \tau) = 1$ , and  $T = M(M^{\sigma, \tau})^{-1}$  is the standard signature of a transducer matchgate by Lemma 4.7. Let  $\underline{R}'_i = \underline{R}_i T^{\otimes m_i}$ , then

$$\underline{R}'_i (M^{\sigma, \tau})^{\otimes m_i} = R_i, \quad \underline{G}_j^{* \leftarrow \sigma, \tau} = (M^{\sigma, \tau})^{\otimes n_j} G_j,$$

for  $1 \leq i \leq r$  and  $1 \leq j \leq g$ , where  $\underline{R}'_i$  and  $\underline{G}_j^{* \leftarrow \sigma, \tau}$  are standard signatures by Lemma 2.1 and Theorem 4.1. This implies that  $R_i, G_j$  are simultaneously realized on the basis  $M^{\sigma, \tau}$  of size 1.  $\square$

## 5 Collapse Theorems on Domain Size 3 and 4

In this section, assume that  $G$  is a generator signature of full rank on domain size  $k \geq 3$ , the basis  $M$  is a  $2^\ell \times k$  matrix of rank  $k$ , and  $\underline{G} = M^{\otimes n} G$  is a standard signature of arity  $n\ell$ . Thus there exists  $t \in [n]$  such that  $\text{rank}(G(t)) = k$ . From Lemma 2.2, we have  $\underline{G}(t) = MG(t)(M^T)^{\otimes (n-1)}$ . Then by Lemma 4.1,  $\text{rank}(\underline{G}(t)) = k$ . Because  $k \geq 3$ , we can define  $\sigma, \tau \in \{0, 1\}^\ell, \zeta, \eta \in \{0, 1\}^{(n-1)\ell}$  as follows:

- $\sigma$  and  $\tau$  have the same parity,
- $\underline{G}(t)^\sigma$  and  $\underline{G}(t)^\tau$  are linearly independent,
- $\text{wt}(\sigma \oplus \tau) = \min_{u \neq v, u, v \in \{0, 1\}^\ell} \{\text{wt}(u \oplus v) \mid \underline{G}(t)^u \text{ and } \underline{G}(t)^v \text{ have the same parity and are linearly independent}\}.$

Let  $x_\beta = \left( \frac{\underline{G}^{\beta \frown_t \sigma}}{\underline{G}^{\beta \frown_t \tau}} \right)$ , then there exist  $\zeta, \eta$  such that:

- $x_\zeta$  and  $x_\eta$  are linearly independent,
- $\text{wt}(\zeta \oplus \eta) = \min_{u \neq v, u, v \in \{0, 1\}^{(n-1)\ell}} \{\text{wt}(u \oplus v) \mid x_u \text{ and } x_v \text{ are linearly independent}\}.$

Then we directly have the following lemma that is similar to Lemma 4.2.

**Lemma 5.1.** *If there exists  $\alpha \in \{0, 1\}^\ell$  that has the same parity as  $\sigma$  such that  $0 < \text{wt}(\sigma \oplus \alpha) < \text{wt}(\sigma \oplus \tau)$  and  $0 < \text{wt}(\alpha \oplus \tau) < \text{wt}(\sigma \oplus \tau)$ , then  $\underline{G}(t)^\alpha$  is identically zero. Similarly, If there exists  $\beta$  such that  $0 < \text{wt}(\eta \oplus \beta) < \text{wt}(\eta \oplus \zeta)$  and  $0 < \text{wt}(\beta \oplus \zeta) < \text{wt}(\eta \oplus \zeta)$ , then  $x_\beta$  is identically zero.*

Let  $\zeta \oplus \eta = e_{q_1} \oplus e_{q_2} \oplus \cdots \oplus e_{q_d}$ , and  $\sigma \oplus \tau = e_{p_1} \oplus e_{p_2} \oplus \cdots \oplus e_{p_d}$ . Then we have the following lemma.

**Lemma 5.2.** *The Hamming distance  $d$  between the minimizing  $\sigma$  and  $\tau$  is 2.*

*Proof.*  $d \neq 1$  since  $\sigma$  and  $\tau$  have the same parity.

For a contradiction assume  $d > 2$ . Let  $x_\zeta = \left( \frac{\underline{G}^{\zeta \frown_t \sigma}}{\underline{G}^{\zeta \frown_t \tau}} \right)$ ,  $x_\eta = \left( \frac{\underline{G}^{\eta \frown_t \sigma}}{\underline{G}^{\eta \frown_t \tau}} \right)$ . These are linearly independent by definition. We will prove that  $\underline{G}^{\zeta \frown_t \sigma} \underline{G}^{\eta \frown_t \tau} - \underline{G}^{\zeta \frown_t \tau} \underline{G}^{\eta \frown_t \sigma} = 0$  by MGI to get a contradiction.

We will apply MGI twice. The first time we use the pattern  $\zeta \curvearrowright_t (\sigma \oplus e_{p_1})$  with the position vector  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2 \cdots p_d)$ . Note that the other pattern obtained by XOR is  $\eta \curvearrowright_t (\tau \oplus e_{p_1})$ . This gives

$$\sum_{i=1}^d (-1)^{i+1} \underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_1} \oplus e_{p_i})} \underline{G}^{\eta \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_i})} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})}). \quad (5.1)$$

The second time we use the same position vector  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2 \cdots p_d)$  with the pattern  $\zeta \curvearrowright_t (\tau \oplus e_{p_1})$ . Note that the other pattern obtained by XOR is  $\eta \curvearrowright_t (\sigma \oplus e_{p_1})$ . This gives

$$\sum_{i=1}^d (-1)^{i+1} \underline{G}^{\zeta \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_i})} \underline{G}^{\eta \curvearrowright_t (\sigma \oplus e_{p_1} \oplus e_{p_i})} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})}), \quad (5.2)$$

Since  $d > 2$ ,  $\underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_1} \oplus e_{p_i})} = 0$ ,  $\underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_1} \oplus e_{p_i})} = 0$  for  $i > 1$  from Lemma 5.1. Then from (5.1) and (5.2) we have

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})}), \quad (5.3)$$

$$\underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})}). \quad (5.4)$$

Note that (5.3) and (5.4) are symmetric for  $\sigma$  and  $\tau$ . By switching  $\sigma$  and  $\tau$ , we will go from (5.3) to (5.4).  $x_\zeta = \begin{pmatrix} \underline{G}^{\zeta \curvearrowright_t \sigma} \\ \underline{G}^{\zeta \curvearrowright_t \tau} \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$  since  $x_\zeta = \begin{pmatrix} \underline{G}^{\zeta \curvearrowright_t \sigma} \\ \underline{G}^{\zeta \curvearrowright_t \tau} \end{pmatrix}$  and  $x_\eta = \begin{pmatrix} \underline{G}^{\eta \curvearrowright_t \sigma} \\ \underline{G}^{\eta \curvearrowright_t \tau} \end{pmatrix}$  are linearly independent. Assume that  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$ . Let the pattern be  $\zeta \curvearrowright_t (\sigma \oplus e_{p_2})$  and the position vector be  $(q_1 \cdots \hat{q}_j \cdots q_{d'}) \curvearrowright_t (p_2 \cdots p_d)$  for  $1 \leq j \leq d'$ , where  $q_1 \cdots \hat{q}_j \cdots q_{d'}$  means deleting  $q_j$  from  $q_1 \cdots q_j \cdots q_{d'}$ . Note that the other pattern obtained by XOR is  $(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_2})$ . Then we have

$$\begin{aligned} & \underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} + \sum_{i=3}^d (-1)^i \underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_2} \oplus e_{p_i})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_2} \oplus e_{p_i})} \\ &= \sum_{1 \leq u \leq d', u \neq j} (\pm \underline{G}^{(\zeta \oplus e_{q_u}) \curvearrowright_t (\sigma \oplus e_{p_2})} \underline{G}^{(\eta \oplus e_{q_j} \oplus e_{q_u}) \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_2})}). \end{aligned}$$

$\underline{G}^{\zeta \curvearrowright_t (\sigma \oplus e_{p_2} \oplus e_{p_i})} = 0$  for  $i > 2$  and  $\underline{G}^{(\eta \oplus e_{q_j} \oplus e_{q_u}) \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_2})} = 0$  from Lemma 5.1, and by assumption  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$ , so  $\underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} = 0$  for  $1 \leq j \leq d'$ . Thus

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} = 0 \quad (5.5)$$

by (5.3).

Furthermore, let the pattern be  $(\zeta \oplus e_{q_j}) \curvearrowright_t \sigma$  and the position vector be  $q_j \curvearrowright_t p_2 p_3 \cdots p_d$  for  $1 \leq j \leq d'$ . The other pattern obtained by XOR is  $\zeta \curvearrowright_t (\tau \oplus e_{p_1})$ . This gives a matchgate identity

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} = \pm \sum_{i=2}^d (-1)^i \underline{G}^{(\zeta \oplus q_j) \curvearrowright_t (\sigma \oplus e_{p_i})} \underline{G}^{\zeta \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_i})}.$$

Since  $\underline{G}^{\zeta \curvearrowright_t (\tau \oplus e_{p_1} \oplus e_{p_i})} = 0$  for  $2 \leq i \leq d$  from Lemma 5.1, and by assumption  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$ , we have  $\underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} = 0$  for  $1 \leq j \leq d'$ . Thus

$$\underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = 0 \quad (5.6)$$

by (5.4).

This implies that  $\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} - \underline{G}^{\eta \curvearrowright_t \sigma} \underline{G}^{\zeta \curvearrowright_t \tau} = 0$  by (5.5) and (5.6). This contradicts that  $x_\zeta = \left( \frac{\underline{G}^{\zeta \curvearrowright_t \sigma}}{\underline{G}^{\zeta \curvearrowright_t \tau}} \right)$  and  $x_\eta = \left( \frac{\underline{G}^{\eta \curvearrowright_t \sigma}}{\underline{G}^{\eta \curvearrowright_t \tau}} \right)$  are linearly independent. Hence  $d = 2$  under the hypothesis  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$ . By symmetry, switching  $\sigma$  and  $\tau$ , we can also prove  $d = 2$  under the hypothesis  $\underline{G}^{\zeta \curvearrowright_t \tau} \neq 0$ .  $\square$

From Lemma 5.2, we have  $\sigma \oplus \tau = e_{p_1} \oplus e_{p_2}$  and  $\zeta \oplus \eta = e_{q_1} \oplus e_{q_2} \oplus \cdots \oplus e_{q_{d'}}$ .

**Lemma 5.3.** *For the given  $\sigma$  and  $\tau$ , the Hamming distance  $d'$  between the minimizing  $\zeta$  and  $\eta$  is 2.*

*Proof.* By the Parity Condition,  $d' \neq 1$ .

For a contradiction assume  $d' > 2$ . Let the pattern be  $\zeta \curvearrowright_t (\sigma \oplus e_{p_1})$  and the position vector be  $(q_1 q_2 \cdots q_{d'}) \curvearrowright_t (p_1 p_2)$ . The other pattern obtained by XOR is  $\eta \curvearrowright_t (\sigma \oplus e_{p_2}) = \eta \curvearrowright_t (\tau \oplus e_{p_1})$ .

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} - \underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = \sum_{j=1}^{d'} (\pm \underline{G}^{(\zeta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})}). \quad (5.7)$$

Since  $x_\zeta = \left( \frac{\underline{G}^{\zeta \curvearrowright_t \sigma}}{\underline{G}^{\zeta \curvearrowright_t \tau}} \right)$  and  $x_\eta = \left( \frac{\underline{G}^{\eta \curvearrowright_t \sigma}}{\underline{G}^{\eta \curvearrowright_t \tau}} \right)$  are linearly independent, we have  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$  or  $\underline{G}^{\eta \curvearrowright_t \sigma} \neq 0$ .

Assume  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$ . Let the pattern be  $\zeta \curvearrowright_t (\sigma \oplus e_{p_2})$  and the position vector be  $(q_1 \cdots \hat{q}_j \cdots q_{d'}) \curvearrowright_t p_2$  for  $1 \leq j \leq d'$ . The other pattern obtained by XOR is  $(\eta \oplus e_{q_j}) \curvearrowright_t \sigma$ . Then from MGI we have

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\sigma \oplus e_{p_2})} = \sum_{1 \leq u \leq d', u \neq j} (\pm \underline{G}^{(\zeta \oplus e_{q_u}) \curvearrowright_t (\sigma \oplus e_{p_2})} \underline{G}^{(\eta \oplus e_{q_u} \oplus e_{q_j}) \curvearrowright_t \sigma}). \quad (5.8)$$

$\underline{G}^{(\eta \oplus e_{q_u} \oplus e_{q_j}) \curvearrowright_t \sigma} = 0$  for  $u \neq j$  by Lemma 5.1, so  $\underline{G}^{(\eta \oplus e_{q_j}) \curvearrowright_t (\tau \oplus e_{p_1})} = 0$  for  $1 \leq j \leq d'$  from (5.8) and  $\tau \oplus e_{p_1} = \sigma \oplus e_{p_2}$ . Then  $\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} - \underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = 0$  from (5.7). This contradicts that  $x_\zeta$  and  $x_\eta$  are linearly independent. Hence  $d' = 2$  under the hypothesis  $\underline{G}^{\zeta \curvearrowright_t \sigma} \neq 0$ . By symmetry, switching  $\zeta$  and  $\eta$ , we can also prove  $d' = 2$  under the hypothesis  $\underline{G}^{\eta \curvearrowright_t \sigma} \neq 0$ .  $\square$

From Lemma 5.2 and Lemma 5.3, we have  $\sigma \oplus \tau = e_{p_1} \oplus e_{p_2}$  and  $\zeta \oplus \eta = e_{q_1} \oplus e_{q_2}$ .

**Theorem 5.1.** *Suppose  $G$  is a generator signature of full rank on domain size  $k \geq 3$  with the  $t$ -th matrix form  $G(t)$  having rank  $k$ . Furthermore suppose there is a basis  $M$  which is a  $2^\ell \times k$  matrix of rank  $k$ , and  $\underline{G} = M^{\otimes n} G$  is a standard signature of arity  $n\ell$ . Then there is a  $4 \times 4$  sub-matrix of rank 4 in  $\underline{G}(t)$ .*

*Proof.* Following the notations of Lemma 5.2 and Lemma 5.3, the sub-matrix  $\begin{pmatrix} \underline{G}^{\zeta \curvearrowright_t \sigma} & \underline{G}^{\eta \curvearrowright_t \sigma} \\ \underline{G}^{\zeta \curvearrowright_t \tau} & \underline{G}^{\eta \curvearrowright_t \tau} \end{pmatrix}$  of  $\underline{G}(t)$  has rank 2, where  $\text{wt}(\sigma \oplus \tau) = 2$  and  $\text{wt}(\eta \oplus \zeta) = 2$ . Let the pattern be  $\zeta \curvearrowright_t (\sigma \oplus e_{p_1})$  and the position vector be  $(q_1 q_2) \curvearrowright_t (p_1 p_2)$ . The other pattern obtained by XOR is  $\eta \curvearrowright_t (\sigma \oplus e_{p_2}) = \eta \curvearrowright_t (\tau \oplus e_{p_1})$ . Then from MGI we have

$$\underline{G}^{\zeta \curvearrowright_t \sigma} \underline{G}^{\eta \curvearrowright_t \tau} - \underline{G}^{\zeta \curvearrowright_t \tau} \underline{G}^{\eta \curvearrowright_t \sigma} = \pm (\underline{G}^{(\zeta \oplus e_{q_1}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_1}) \curvearrowright_t (\tau \oplus e_{p_1})} - \underline{G}^{(\zeta \oplus e_{q_2}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_2}) \curvearrowright_t (\tau \oplus e_{p_1})}).$$

It is “+” if  $q_1 < p_1 < p_2 < q_2$ . Otherwise, it is “-”, when  $q_1 < q_2 < p_1 < p_2$  or  $p_1 < p_2 < q_1 < q_2$ . Thus

$$\underline{G}^{(\zeta \oplus e_{q_1}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_1}) \curvearrowright_t (\tau \oplus e_{p_1})} - \underline{G}^{(\zeta \oplus e_{q_2}) \curvearrowright_t (\sigma \oplus e_{p_1})} \underline{G}^{(\eta \oplus e_{q_2}) \curvearrowright_t (\tau \oplus e_{p_1})} \neq 0. \quad (5.9)$$

By renaming  $\sigma$  and  $\tau$ , the  $p_1, p_2$ -th bits of  $\sigma$  can be 00 or 01 (and the  $p_1, p_2$ -th bits of  $\tau$  are 11 or 10 correspondingly). Similarly by renaming  $\zeta$  and  $\eta$ , the  $q_1, q_2$ -th bits of  $\zeta$  can be 00 or 01 (and the  $q_1, q_2$ -th bits of  $\eta$  are 11 or 10 correspondingly). So there are four cases for the  $q_1, q_2$ -th,  $p_1, p_2$ -th bits of  $\zeta \curvearrowright_t \sigma$ . We may temporarily make the assumption that  $q_1, q_2$ -th,  $p_1, p_2$ -th bits of  $\zeta \curvearrowright_t \sigma$  are 00, 00 respectively. Then  $\underline{G}(t)$  has a full rank sub-matrix of the following form by (5.9):

$$\begin{pmatrix} \underline{G}^{\zeta \curvearrowright_t \sigma} & 0 & 0 & \underline{G}^{\eta \curvearrowright_t \sigma} \\ 0 & \underline{G}^{(\zeta \oplus e_{q_2}) \curvearrowright_t (\sigma \oplus e_{p_2})} & \underline{G}^{(\zeta \oplus e_{q_1}) \curvearrowright_t (\sigma \oplus e_{p_2})} & 0 \\ 0 & \underline{G}^{(\zeta \oplus e_{q_2}) \curvearrowright_t (\sigma \oplus e_{p_1})} & \underline{G}^{(\zeta \oplus e_{q_1}) \curvearrowright_t (\sigma \oplus e_{p_1})} & 0 \\ \underline{G}^{\zeta \curvearrowright_t \tau} & 0 & 0 & \underline{G}^{\eta \curvearrowright_t \tau} \end{pmatrix}. \quad (5.10)$$

If the  $q_1, q_2$ -th,  $p_1, p_2$ -th bits of  $\zeta \curvearrowright_t \sigma$  are 00, 01, then the full rank sub-matrix has the following form by (5.9):

$$\begin{pmatrix} 0 & \underline{G}^{(\zeta \oplus e_{q_2}) \curvearrowright_t (\sigma \oplus e_{p_2})} & \underline{G}^{(\zeta \oplus e_{q_1}) \curvearrowright_t (\sigma \oplus e_{p_2})} & 0 \\ \underline{G}^{\zeta \curvearrowright_t \sigma} & 0 & 0 & \underline{G}^{\eta \curvearrowright_t \sigma} \\ \underline{G}^{\zeta \curvearrowright_t \tau} & 0 & 0 & \underline{G}^{\eta \curvearrowright_t \tau} \\ 0 & \underline{G}^{(\zeta \oplus e_{q_2}) \curvearrowright_t (\sigma \oplus e_{p_1})} & \underline{G}^{(\zeta \oplus e_{q_1}) \curvearrowright_t (\sigma \oplus e_{p_1})} & 0 \end{pmatrix}. \quad (5.11)$$

If the  $q_1, q_2$ -th,  $p_1, p_2$ -th bits of  $\zeta \curvearrowright_t \sigma$  are 01, 00, then we get the full rank sub-matrix by switching  $\zeta$  with  $\zeta \oplus e_{q_2}$  and  $\sigma$  with  $\sigma \oplus e_{p_2}$  in (5.11).

If the  $q_1, q_2$ -th,  $p_1, p_2$ -th bits of  $\zeta \curvearrowright_t \sigma$  are 01, 01, then we get the full rank sub-matrix by switching  $\zeta$  with  $\zeta \oplus e_{q_2}$  and  $\sigma$  with  $\sigma \oplus e_{p_2}$  in (5.10).  $\square$

**Corollary 5.1.** *Let  $\underline{G}$  be a standard signature and  $\underline{G}(t)$  be the  $t$ -th matrix form of  $\underline{G}$ . If there are two rows with the same parity that are linearly independent in  $\underline{G}(t)$ , then  $\text{rank}(\underline{G}(t)) \geq 4$ .*

**Remark 4.** *If  $\underline{G}(t)$  has rank  $k \geq 3$ , then there are some two rows, of the same parity, that are linearly independent.*

**Corollary 5.2.** *If there exists  $t \in [k]$  such that  $\text{rank}(G(t)) = 3$  and  $M$  is a  $2^\ell \times k$  matrix of rank  $k$ , then  $G$  cannot be realized on  $M$ .*

*Proof.* If  $\underline{G} = M^{\otimes n} G$ , then  $\underline{G}(t) = M G(t) (M^T)^{\otimes (n-1)}$  and  $\text{rank}(\underline{G}(t)) = 3$  by Lemma 4.1. So there are two rows that have the same parity and are linearly independent in  $\underline{G}(t)$ . Then by Corollary 5.1,  $\text{rank}(\underline{G}(t)) \geq 4$ . This is a contradiction, so  $G$  cannot be realized on any full rank basis.  $\square$

## 5.1 A Collapse Theorem on Domain Size 3

From Corollary 5.2, we directly have the following Theorem:

**Theorem 5.2.** *Let  $G$  be a full rank generator signature on domain size 3, then it cannot be realized on a basis of rank 3.*

**Remark 5.** *So for generator signatures on domain size 3, the only way to be realizable by a full ranked matchgate is via a basis of rank 2.*

In paper [14], the following result about holographic algorithms on bases of rank 2 is given:



**Theorem 5.3.** Let  $R_1, R_2, \dots, R_r$  and  $G_1, G_2, \dots, G_g$  be the recognizer and generator signatures on domain size  $k \geq 3$  that a holographic algorithm employs. If  $R_1, R_2, \dots, R_r$  and  $G_1, G_2, \dots, G_g$  can be realized on a  $2^\ell \times k$  basis  $M$  of rank 2, where  $\ell \geq 2$ , then we can efficiently find signatures  $R'_1, R'_2, \dots, R'_r$  and  $G'_1, G'_2, \dots, G'_g$  on domain size 2 such that the contraction of  $\bigotimes_{i=1}^g G'_i$  and  $\bigotimes_{j=1}^r R'_j$  is equal to the contraction of  $\bigotimes_{i=1}^g G_i$  and  $\bigotimes_{j=1}^r R_j$ . And if there is at least one full rank generator signature  $G'_i$ , then  $R_1, R_2, \dots, R_r$  and  $G_1, G_2, \dots, G_g$  can be simultaneously realized on a  $2 \times k$  basis (of size 1).

**Remark 6.** Since  $G'_1, G'_2, \dots, G'_g$  are signatures on domain size 2, either they are all degenerate or there is some  $G'_i$  that is of full rank by Definition 3.1 and Definition 3.2. If  $G'_1, G'_2, \dots, G'_g$  are all degenerate, then the contraction of  $\bigotimes_{i=1}^g G'_i$  and  $\bigotimes_{j=1}^r R'_j$  can be computed trivially in polynomial time. And since the contraction of  $\bigotimes_{i=1}^g G'_i$  and  $\bigotimes_{j=1}^r R'_j$  is same as the contraction of  $\bigotimes_{i=1}^g G_i$  and  $\bigotimes_{j=1}^r R_j$ , the holographic algorithm can be computed trivially in polynomial time. Otherwise we have the following collapse theorem for holographic algorithms on domain size 3.

**Theorem 5.4.** On domain size 3, for any holographic algorithm using a set of signatures  $R_1, R_2, \dots, R_r$  and  $G_1, G_2, \dots, G_g$ , and a  $2^\ell \times 3$  basis  $M$  of size  $\ell \geq 2$  on which these signatures are simultaneously realized by matchgates, we can efficiently replace the signatures with an equivalent set having the same Holant value. And for the new set of signatures, we can efficiently decide whether it is a degenerate set, i.e., all generators are degenerate, in which case we can compute the Holant in polynomial time trivially, or else, we can efficiently find another  $2 \times 3$  basis  $M'$  (of size 1), on which  $R_1, R_2, \dots, R_r$  and  $G_1, G_2, \dots, G_g$  can be simultaneously realized. Thus, any non-trivial holographic algorithm using matchgates on domain size 3 can be accomplished by a basis of size 1.

## 5.2 A Group Property of Standard Signatures

**Lemma 5.4.** Assume that

$$A = \begin{pmatrix} G^{0000} & 0 & 0 & G^{0011} \\ 0 & G^{0101} & G^{0110} & 0 \\ 0 & G^{1001} & G^{1010} & 0 \\ G^{1100} & 0 & 0 & G^{1111} \end{pmatrix}$$

has rank 4 and

$$G^{0000}G^{1111} - G^{1100}G^{0011} = \pm(G^{1010}G^{0101} - G^{1001}G^{0110}), \quad (5.12)$$

then  $G^{-1}$  is of the following form

$$G^{-1} = \begin{pmatrix} g^{0000} & 0 & 0 & g^{0011} \\ 0 & g^{0101} & g^{0110} & 0 \\ 0 & g^{1001} & g^{1010} & 0 \\ g^{1100} & 0 & 0 & g^{1111} \end{pmatrix}$$

and

$$g^{0000}g^{1111} - g^{1100}g^{0011} = \pm(g^{1010}g^{0101} - g^{1001}g^{0110}),$$

with the same sign  $\pm$  as in (5.12).

*Proof.* Note that  $\begin{pmatrix} G^{0000} & G^{0011} \\ G^{1100} & G^{1111} \end{pmatrix}$  and  $\begin{pmatrix} G^{0101} & G^{0110} \\ G^{1001} & G^{1010} \end{pmatrix}$  have rank 2. Let

$$\begin{pmatrix} g^{0000} & g^{0011} \\ g^{1100} & g^{1111} \end{pmatrix} = \begin{pmatrix} G^{0000} & G^{0011} \\ G^{1100} & G^{1111} \end{pmatrix}^{-1}, \quad \begin{pmatrix} g^{0101} & g^{0110} \\ g^{1001} & g^{1010} \end{pmatrix} = \begin{pmatrix} G^{0101} & G^{0110} \\ G^{1001} & G^{1010} \end{pmatrix}^{-1},$$

then

$$G^{-1} = \begin{pmatrix} g^{0000} & 0 & 0 & g^{0011} \\ 0 & g^{0101} & g^{0110} & 0 \\ 0 & g^{1001} & g^{1010} & 0 \\ g^{1100} & 0 & 0 & g^{1111} \end{pmatrix}$$

and

$$\begin{aligned} g^{0000}g^{1111} - g^{1100}g^{0011} &= (G^{0000}G^{1111} - G^{1100}G^{0011})^{-1}, \\ g^{1010}g^{0101} - g^{1001}g^{0110} &= (G^{1010}G^{0101} - G^{1001}G^{0110})^{-1}. \end{aligned}$$

Thus

$$g^{0000}g^{1111} - g^{1100}g^{0011} = \pm(g^{1010}g^{0101} - g^{1001}g^{0110}).$$

□

Similarly, we have the following Lemma.

**Lemma 5.5.** *Assume that*

$$A = \begin{pmatrix} 0 & G^{0001} & G^{0010} & 0 \\ G^{0100} & 0 & 0 & G^{0111} \\ G^{1000} & 0 & 0 & G^{1011} \\ 0 & G^{1101} & G^{1110} & 0 \end{pmatrix}$$

has rank 4 and

$$G^{1000}G^{0111} - G^{0100}G^{1011} = \pm(G^{0010}G^{1101} - G^{0001}G^{1110}), \quad (5.13)$$

then  $G^{-1}$  is of the following form

$$G^{-1} = \begin{pmatrix} 0 & g^{0001} & g^{0010} & 0 \\ g^{0100} & 0 & 0 & g^{0111} \\ g^{1000} & 0 & 0 & g^{1011} \\ 0 & g^{1101} & g^{1110} & 0 \end{pmatrix}$$

and

$$g^{1000}g^{0111} - g^{0100}g^{1011} = \pm(g^{0010}g^{1101} - g^{0001}g^{1110}),$$

with the same sign  $\pm$  as in (5.13).

**Remark 7.** In fact, Lemma 5.4 and Lemma 5.5 are the group properties of standard signatures of arity 4, where  $\pm$  is due to the exact ordering of the 4 bits when we defined the matrix relative to MGI.

**Theorem 5.5.** Let  $\underline{G} = (\underline{G}^{\alpha_1\alpha_2\cdots\alpha_n})$  be the standard signature of a generator matchgate  $\Gamma$  of arity  $2n$ . If  $\underline{G}$  has full rank and the  $t$ -th matrix form  $\underline{G}(t)$  has rank 4, then there exists a standard signature  $\underline{R}$  realized by a recognizer matchgate of arity  $2n$  such that  $\underline{G}(t)\underline{R}(t) = I_4$ .

*Proof.* We follow the notations of Lemma 5.2 and Lemma 5.3. From Theorem 5.1, there is a sub-matrix of rank 4

$$A = \begin{pmatrix} \underline{G}^{\alpha\curvearrowright_t 00} & \underline{G}^{\beta\curvearrowright_t 00} & \underline{G}^{\gamma\curvearrowright_t 00} & \underline{G}^{\delta\curvearrowright_t 00} \\ \underline{G}^{\alpha\curvearrowright_t 01} & \underline{G}^{\beta\curvearrowright_t 01} & \underline{G}^{\gamma\curvearrowright_t 01} & \underline{G}^{\delta\curvearrowright_t 01} \\ \underline{G}^{\alpha\curvearrowright_t 10} & \underline{G}^{\beta\curvearrowright_t 10} & \underline{G}^{\gamma\curvearrowright_t 10} & \underline{G}^{\delta\curvearrowright_t 10} \\ \underline{G}^{\alpha\curvearrowright_t 11} & \underline{G}^{\beta\curvearrowright_t 11} & \underline{G}^{\gamma\curvearrowright_t 11} & \underline{G}^{\delta\curvearrowright_t 11} \end{pmatrix}$$

in  $\underline{G}(t)$ , where the  $q_1, q_2$ -th bits of  $\alpha, \beta, \gamma, \delta$  are 00, 01, 10, 11 respectively, and all other bits are the same.

By the Parity Condition,  $A$  is of the form

$$A = \begin{pmatrix} \underline{G}^{\alpha \curvearrowright t 00} & 0 & 0 & \underline{G}^{\delta \curvearrowright t 00} \\ 0 & \underline{G}^{\beta \curvearrowright t 01} & \underline{G}^{\gamma \curvearrowright t 01} & 0 \\ 0 & \underline{G}^{\beta \curvearrowright t 10} & \underline{G}^{\gamma \curvearrowright t 10} & 0 \\ \underline{G}^{\alpha \curvearrowright t 11} & 0 & 0 & \underline{G}^{\delta \curvearrowright t 11} \end{pmatrix} \quad (5.14)$$

or

$$A = \begin{pmatrix} 0 & \underline{G}^{\beta \curvearrowright t 00} & \underline{G}^{\gamma \curvearrowright t 00} & 0 \\ \underline{G}^{\alpha \curvearrowright t 01} & 0 & 0 & \underline{G}^{\delta \curvearrowright t 01} \\ \underline{G}^{\alpha \curvearrowright t 10} & 0 & 0 & \underline{G}^{\delta \curvearrowright t 10} \\ 0 & \underline{G}^{\beta \curvearrowright t 11} & \underline{G}^{\gamma \curvearrowright t 11} & 0 \end{pmatrix}. \quad (5.15)$$

We prove Theorem 5.5 for the case in (5.14). The other case is similar.

Let the position vector be  $(q_1 q_2) \curvearrowright (p_1 p_2)$  and the pattern be  $\alpha \curvearrowright t 10$ , then we have from MGI

$$\underline{G}^{\alpha \curvearrowright t 00} \underline{G}^{\delta \curvearrowright t 11} - \underline{G}^{\alpha \curvearrowright t 11} \underline{G}^{\delta \curvearrowright t 00} = \pm (\underline{G}^{\gamma \curvearrowright t 10} \underline{G}^{\beta \curvearrowright t 01} - \underline{G}^{\beta \curvearrowright t 10} \underline{G}^{\gamma \curvearrowright t 01}).$$

It is “+” if  $q_1 < p_1 < p_2 < q_2$ . Otherwise it is “−”.

Let  $\underline{R}$  be a vector of dimension  $2^{2n}$ , where

$$\begin{pmatrix} \underline{R}_{\alpha \curvearrowright t 00} & 0 & 0 & \underline{R}_{\alpha \curvearrowright t 11} \\ 0 & \underline{R}_{\beta \curvearrowright t 01} & \underline{R}_{\beta \curvearrowright t 10} & 0 \\ 0 & \underline{R}_{\gamma \curvearrowright t 01} & \underline{R}_{\gamma \curvearrowright t 10} & 0 \\ \underline{R}_{\delta \curvearrowright t 00} & 0 & 0 & \underline{R}_{\delta \curvearrowright t 11} \end{pmatrix} = A^{-1},$$

and all other entries of  $\underline{R}$  are zero. It is obvious that  $\underline{G}(t)\underline{R}(t) = I_4$ . Furthermore, by Lemma 5.4,  $\underline{R}$  satisfies

$$\underline{R}_{\alpha \curvearrowright t 00} \underline{R}_{\delta \curvearrowright t 11} - \underline{R}_{\alpha \curvearrowright t 11} \underline{R}_{\delta \curvearrowright t 00} = \pm (\underline{R}_{\gamma \curvearrowright t 10} \underline{R}_{\beta \curvearrowright t 01} - \underline{R}_{\beta \curvearrowright t 10} \underline{R}_{\gamma \curvearrowright t 01}).$$

It is “+” if  $q_1 < p_1 < p_2 < q_2$ . Otherwise is “−”. Note that this is the only non-trivial matchgate identity for  $\underline{R}$ . Thus  $\underline{R}$  is a standard signature realized by a recognizer matchgate by Lemma 2.2.  $\square$

### 5.3 A Collapse Theorem on Domain Size 4

In this subsection, assume that  $G$  is a generator signature of full rank on domain size 4, the basis  $M$  is a  $2^\ell \times 4$  matrix of rank 4, and  $\underline{G} = M^{\otimes n} G$  is a standard signature of arity  $n\ell$ . Since  $G$  is a signature of full rank on domain size 4, there exists  $t \in [n]$  such that  $\text{rank}(G(t)) = 4$ . Following the notations of Lemma 5.2 and Lemma 5.3, denote  $\{\sigma, \sigma \oplus e_{p_1}, \sigma \oplus e_{p_2}, \sigma \oplus e_{p_1} \oplus e_{p_2}\}$  as  $\sigma + \{e_{p_1}, e_{p_2}\}$ . Note that  $\sigma \oplus e_{p_1} \oplus e_{p_2} = \tau$ .

**Lemma 5.6.**  $M^{\sigma + \{e_{p_1}, e_{p_2}\}}$  is invertible.

*Proof.* Note that the sub-matrix of rank 4 in the proof of Theorem 5.1 is a sub-matrix of  $M^{\sigma + \{e_{p_1}, e_{p_2}\}}$   $G(t)(M^T)^{\otimes(n-1)}$ , so  $M^{\sigma + \{e_{p_1}, e_{p_2}\}}$  has rank at least 4. Furthermore, note that  $M^{\sigma + \{e_{p_1}, e_{p_2}\}}$  is a  $4 \times 4$  matrix, so  $M^{\sigma + \{e_{p_1}, e_{p_2}\}}$  is invertible.  $\square$

Note that  $(M^{\sigma + \{e_{p_1}, e_{p_2}\}})^{\otimes n} G$  is a column vector of dimension  $2^{2n}$  and we denote it by  $\underline{G}^{* \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}$ .

**Theorem 5.6.**  $\underline{G}^{* \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}} = (M^{\sigma + \{e_{p_1}, e_{p_2}\}})^{\otimes n} G$  is the standard signature of a generator matchgate of arity  $2n$  and  $\underline{G}^{* \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}(t)$  has rank 4.

*Proof.* Let  $\Gamma$  be a matchgate realizing the standard signature  $\underline{G} = M^{\otimes n}G$ . Note that  $\Gamma$  has  $n\ell$  external nodes. For every block of  $\ell$  nodes, we add an edge of weight 1 to the  $i$ -th external node if the  $i$ -th bit of  $\alpha$  is 1 and do nothing to it if the  $i$ -th bit of  $\alpha$  is 0 for  $1 \leq i \leq \ell$ . Then we get a new matchgate  $\Gamma'$ . Furthermore, for every block of  $\Gamma'$ , view the  $p_1, p_2$ -th external nodes as external nodes and all others as internal nodes, we get a matchgate realizing  $\underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}} = (M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes n}G$ . Since  $M^{\sigma+\{e_{p_1}, e_{p_2}\}}$  has rank 4,  $\underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}(t) = M^{\sigma+\{e_{p_1}, e_{p_2}\}}G(t)((M^{\sigma+\{e_{p_1}, e_{p_2}\}})^T)^{\otimes(n-1)}$  has rank 4.  $\square$

Note that  $(M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes(t-1)} \otimes M \otimes (M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes(n-t)} \cdot G$  is a column vector of dimension  $2^{2n+\ell-2}$  and denote it by  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}$ .

**Lemma 5.7.**  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}} = (M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes(t-1)} \otimes M \otimes (M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes(n-t)} G$  is the standard signature of a generator matchgate of arity  $2n + \ell - 2$ .

*Proof.* Let  $\Gamma$  be a matchgate realizing the standard signature  $\underline{G} = M^{\otimes n}G$ . Note that  $\Gamma$  has  $n\ell$  external nodes. We do nothing to the  $t$ -th block. For other blocks, we add an edge of weight 1 to the  $i$ -th external node if the  $i$ -th bit of  $\alpha$  is 1 and do nothing to it if the  $i$ -th bit of  $\alpha$  is 0 for  $1 \leq i \leq \ell$ . Then we get a new matchgate  $\Gamma'$ . The external nodes of  $\Gamma'$  consists of the external nodes in the  $t$ -th block, and the  $p_1, p_2$ -th external nodes in the other blocks, then we get a matchgate realizing  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}$ .  $\square$

Let  $T = M(M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{-1}$  (Note that  $T^{\sigma+\{e_{p_1}, e_{p_2}\}} = I_4$ ), then

$$\underline{G} = M^{\otimes n}G = T^{\otimes n}(M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes n}G = T^{\otimes n}\underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}$$

and

$$\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}} = (T^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes(t-1)} \otimes T \otimes (T^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes(n-t)} \underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}.$$

The entries of  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}$  can be indexed by  $i_{1,1}i_{1,2} \cdots i_{t-1,1}i_{t-1,2}i'_1 \cdots i'_\ell i_{t+1,1}i_{t+1,2} \cdots i_{n,1}i_{n,2} \in \{0, 1\}^{2n+\ell-2}$ . Denote the matrix form of  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}$  whose rows are indexed by  $i'_1 \cdots i'_\ell$  and columns indexed by  $i_{1,1}i_{1,2} \cdots i_{t-1,1}i_{t-1,2}i_{t+1,1}i_{t+1,2} \cdots i_{n,1}i_{n,2}$  as  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}(t)$ , then

$$\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}(t) = T \underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}(t) ((T^{\sigma+\{e_{p_1}, e_{p_2}\}})^T)^{\otimes(n-1)} = T \underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}(t). \quad (5.16)$$

**Lemma 5.8.**  $T$  is the standard signature of a transducer matchgate of  $\ell$ -output and 2-input.

*Proof.* By Theorem 5.5 and Theorem 5.6, there exists a standard signature  $\underline{R}$  realized by a recognizer matchgate of arity  $2n$  such that  $\underline{G}^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}(t)\underline{R}(t) = I_4$  (Note that  $\underline{R}(t)$  is a  $2^{2n-2} \times 4$  matrix). Let  $\Gamma_1$  be the matchgate realizing  $\underline{G}^{t^c \leftarrow \sigma + \{e_{p_1}, e_{p_2}\}}$  with output nodes  $X_{1,1}, X_{1,2}, \dots, X_{t-1,1}, X_{t-1,2}, Y_1, Y_2, \dots, Y_\ell, Z_{t+1,1}, Z_{t+1,2}, \dots, Z_{n,1}, Z_{n,2}$ , and  $\Gamma_2$  be the matchgate realizing  $\underline{R}$  with input nodes  $W_{1,1}, W_{1,2}, W_{2,1}, W_{2,2}, \dots, W_{n,1}, W_{n,2}$ . Connect  $X_{i,1}$  with  $W_{i,1}$ ,  $X_{i,2}$  with  $W_{i,2}$ , for  $1 \leq i \leq t-1$  and  $Z_{i,1}$  with  $W_{i,1}$ ,  $Z_{i,2}$  with  $W_{i,2}$ , for  $t+1 \leq i \leq n$  by an edge with weight 1 respectively, then we get a transducer matchgate  $\Gamma$  with output nodes  $Y_1, Y_2, \dots, Y_\ell$  and input nodes  $W_{t,1}, W_{t,2}$ . And  $T = \underline{G}^{t^c \leftarrow \sigma, \tau}(t)\underline{R}(t)$  is the standard signature of  $\Gamma$ .  $\square$

The proof of Lemma 5.8 is illustrated by Fig. 2.

**Theorem 5.7.** Any holographic algorithm on a basis of size  $\ell$  and domain size 4 which employs at least one generator signature of full rank can be simulated on a basis of size 2.

*Proof.* Let  $\underline{R}_i M^{\otimes m_i} = R_i$  for  $1 \leq i \leq r$  and  $\underline{G}_j = M^{\otimes n_j}G_j$  for  $1 \leq j \leq g$ , where  $R_i, G_j$  are recognizer and generator signatures that a holographic algorithm employs and  $\underline{R}_i, \underline{G}_j$  are standard signatures. Without loss of generality, let  $G_1$  be of full rank, and  $\underline{G}_1 = M^{\otimes n_1}G_1$ . Starting from  $G_1$  we define  $\sigma$

and  $\tau$ . Then the basis  $M$  has a full rank sub-matrix  $M^{\sigma+\{e_{p_1}, e_{p_2}\}}$  and  $T = M(M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{-1}$  is the standard signature of a transducer matchgate. Let  $\underline{R}'_i = \underline{R}_i T^{\otimes m_i}$ , then

$$\underline{R}'_i(M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes m_i} = R_i, \quad \underline{G}_j^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}} = (M^{\sigma+\{e_{p_1}, e_{p_2}\}})^{\otimes n_j} G_j,$$

for  $1 \leq i \leq r$ ,  $1 \leq j \leq g$ , where  $\underline{R}'_i$  and  $\underline{G}_j^{*\leftarrow\sigma+\{e_{p_1}, e_{p_2}\}}$  are standard signatures by Lemma 2.1 and Theorem 5.6. This implies that  $R_i, G_j$  are simultaneously realized on the basis  $M^{\sigma+\{e_{p_1}, e_{p_2}\}}$ .  $\square$

## 6 Acknowledgments

We would like to thank Pinyan Lu, Tyson Williams, Heng Guo, Leslie Valiant for their interest and especially Tyson Williams for his computer code in our experimentation.

## References

- [1] Rodney J. Baxter: *Exactly solved models in statistical mechanics*, Academic Press Inc. (1982). ISBN 978-0-12-083180-7, MR690578.
- [2] Andrei A. Bulatov: The Complexity of the Counting Constraint Satisfaction Problem. ICALP (1) 2008: 646-661
- [3] J-Y Cai and Pinyan Lu: Holographic algorithms: The power of dimensionality resolved. Theor. Comput. Sci. 410(18): 1618-1628 (2009). A preliminary version appeared in ICALP 2007: 631-642. *Best Paper Award*.
- [4] J-Y. Cai and Pinyan Lu. Holographic Algorithms: From Art to Science. J. Computer and System Sciences 77(2011), 41-61. A preliminary version appeared in STOC 2007: 401-410.
- [5] Jin-Yi Cai, Pinyan Lu and Mingji Xia. Holographic algorithms with matchgates capture precisely tractable planar  $\#CSP$ . In *FOCS*, pages 427–436. IEEE Computer Society, 2010.
- [6] Jin-Yi Cai, Xi Chen and Pinyan Lu: Graph Homomorphisms with Complex Values: A Dichotomy Theorem. ICALP (1) 2010: 275-286 CoRR abs/0903.4728 (2009) (To appear in SIAM J Comp.)
- [7] Jin-Yi Cai and Xi Chen: Complexity of counting CSP with complex weights. STOC 2012: 909-920
- [8] Jin-Yi Cai, Michael Kowalczyk and Tyson Williams: Gadgets and anti-gadgets leading to a complexity dichotomy. ITCS 2012: 452-467
- [9] Jin-Yi Cai, Heng Guo and Tyson Williams. A complete dichotomy rises from the capture of vanishing signatures. *CoRR*, abs/1204.6445, 2012. To appear in *STOC*, ACM, 2013.
- [10] Jin-Yi Cai and Michael Kowalczyk: Spin systems on  $k$ -regular graphs with complex edge functions. Theor. Comput. Sci. 461: 2-16 (2012)
- [11] Jin-Yi Cai and Aaron Gorenstein: Matchgates Revisited. <http://arxiv.org/abs/1303.6729>. In submission.
- [12] Martin E. Dyer and David Richerby: On the complexity of  $\#CSP$ . STOC 2010: 725-734
- [13] Martin E. Dyer, Leslie Ann Goldberg and Mark Jerrum: The Complexity of Weighted Boolean CSP. SIAM J. Comput. 38(5): 1970-1986 (2009)
- [14] Zhiguo Fu, Fengqin Yang: Holographic Algorithms on bases of rank 2. <http://arxiv.org/abs/1303.7361>. In submission.
- [15] Leslie Ann Goldberg, Martin Grohe, Mark Jerrum and Marc Thurley: A Complexity Dichotomy for Partition Functions with Mixed Signs. SIAM J. Comput. 39(7): 3336-3402 (2010)
- [16] Heng Guo, Pinyan Lu and Leslie G. Valiant. The Complexity of Symmetric Boolean Parity Holant Problems. ICALP (1) 2011: 712-723.

- [17] Heng Guo and Tyson Williams: The Complexity of Planar Boolean  $\#$ CSP with Complex Weights. CoRR abs/1212.2284 (2012)
- [18] P. W. Kasteleyn, The statistics of dimmers on a lattice, *Physica* 27 (1961) 1209-1225.
- [19] P. W. Kasteleyn, Graph Theory and Crystal Physics. In *Graph Theory and Theoretical Physics*, (F. Harary, ed.), Academic Press, London, 43-110 (1967).
- [20] H. N. V. Temperley and M. E. Fisher. Dimer problem in statistical mechanics - an exact result. *Philosophical Magazine* 6: 1061- 1063 (1961).
- [21] L. G. Valiant. Quantum circuits that can be simulated classically in polynomial time. *SIAM Journal of Computing*, 31(4): 1229-1254 (2002). A preliminary version appeared in *STOC 2001*: 114-123.
- [22] L. G. Valiant. Holographic Algorithms, *SIAM J. on Computing*, 37:5 (2008) 1565-1594. A preliminary version appeared in *FOCS 2004*: 306-315.
- [23] L. G. Valiant. Accidental Algorithms. In *Proc. 47th Annual IEEE Symposium on Foundations of Computer Science 2006*, 509-517.
- [24] L. G. Valiant. Some observations on holographic algorithms, *Proc. 9th Latin American Theoretical Informatics Symposium, LATIN 2010. LNCS, Vol 6034 Springer-Verlag (2010)*, 577-590.
- [25] M. Xia, P. Zhang and W. Zhao: Computational complexity of counting problems on 3-regular planar graphs. *Theor. Comput. Sci.* 384(1) (2007) 111-125.

# Figures

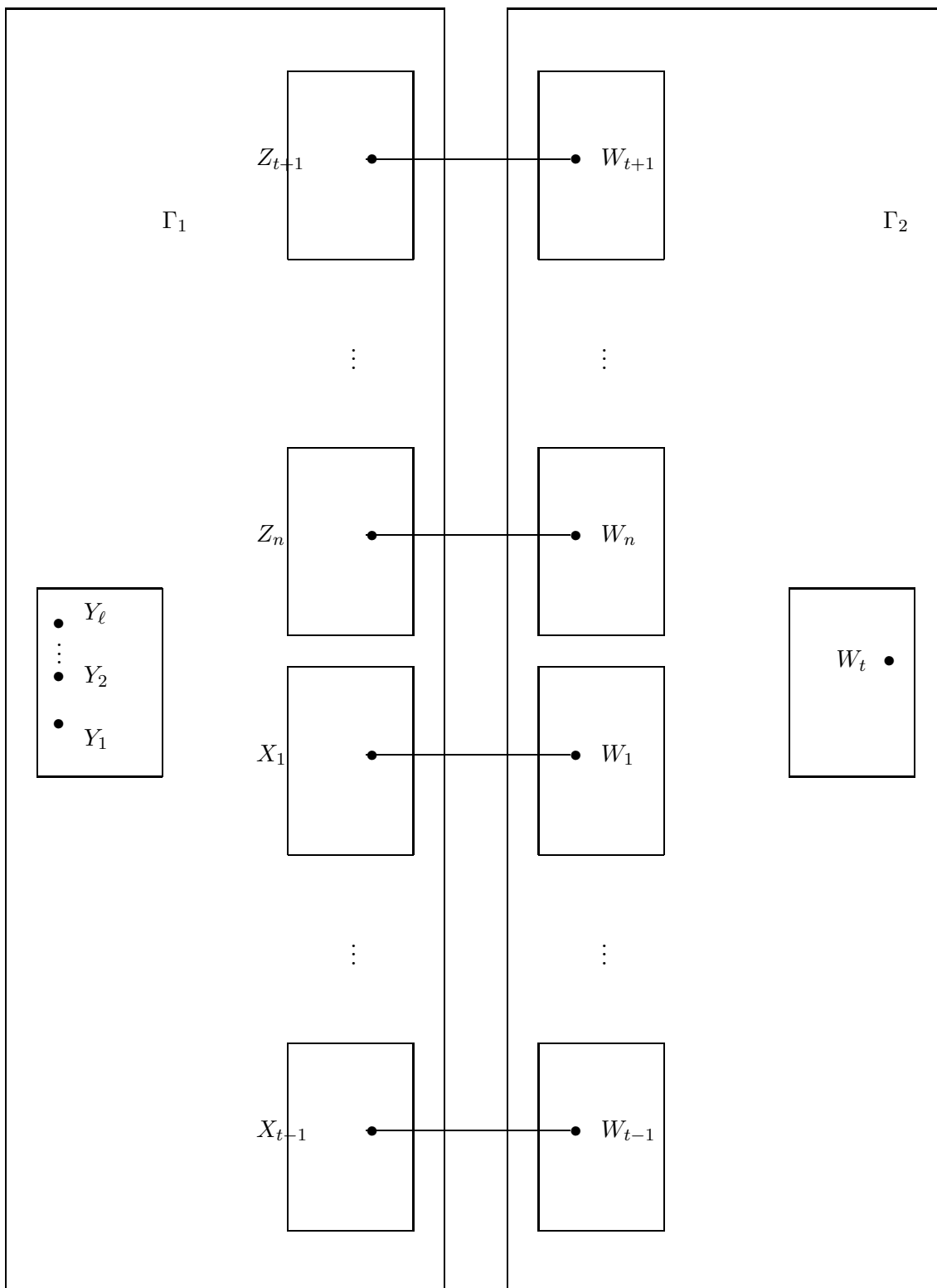


Fig. 1  
22

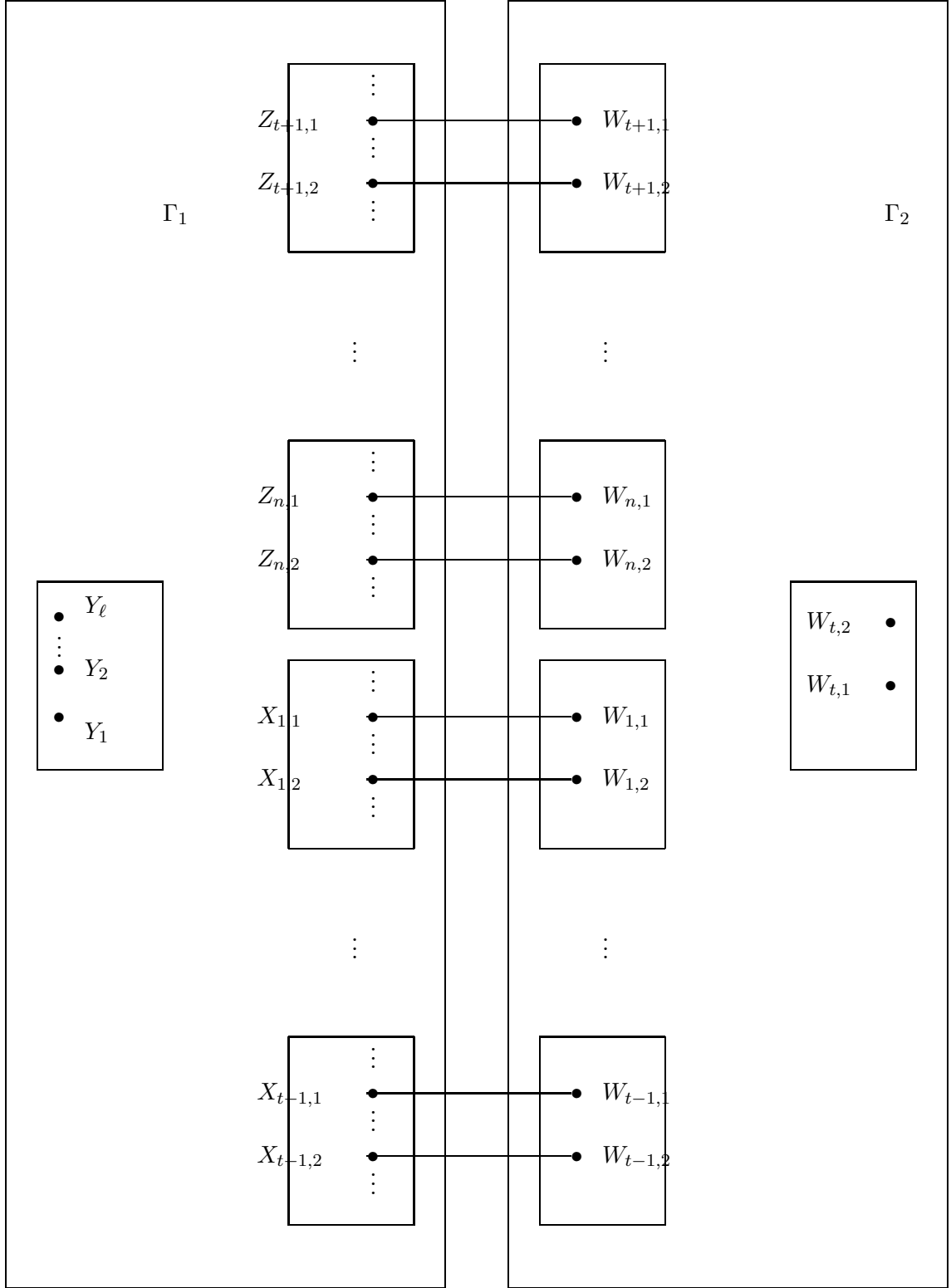


Fig. 2



## Appendix

We consider the following problem on domain size 4 as an illustration of problems solved by holographic algorithms using matchgates.

### Doppler Shift Problem

**Input:** An undirected 3-regular graph  $G$ .

**Output:** The number of {Red, Yellow, Green, Blue}-colorings of the edges of  $G$ , such that at every vertex, either there is a *Red-shift*, namely all incident edges are colored with Red or Yellow, or Green, but not Blue, or there is a *Blue-shift*, namely all incident edges are colored with Blue, or Green, or Yellow, but not Red.

We consider the following basis  $M \in \mathbb{C}^{4 \times 4}$ , where

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

If we index the rows and columns of  $M$  by  $x_1x_2 \in \{0,1\}^2$  and  $y_1y_2 \in \{0,1\}^2$  respectively, then the entry indexed by  $(x_1x_2, y_1y_2)$  is  $(-1)^{x_1y_2+x_2y_1}$ . If we identify 00, 01, 10, 11 with the colors Red, Yellow, Green, Blue, respectively, then it can be directly verified that an arity 3 function on domain  $\{0,1\}^2$  representing the local constraint of this problem under the holographic transformation of  $M^{\otimes 3}$  can be realized by a matchgate of arity 6. As this  $M$  is (a scalar multiple of) an orthogonal matrix, we see that this problem can be solved by matchgates in polynomial time after the holographic transformation.